Fordham International Law Journal

Volume 21, *Issue* 3 1997 *Article* 8

Encrypted Digital Cash Transfers: Why Traditional Money Laundering Controls May Fail Without Uniform Cryptography Regulations

Christopher D. Hoffman*

*

Encrypted Digital Cash Transfers: Why Traditional Money Laundering Controls May Fail Without Uniform Cryptography Regulations

Christopher D. Hoffman

Abstract

This Note argues that key escrow represents a solution to the problem of digital money laundering. In addition, this Note argues that the European Commission has wrongly concluded that key escrow should develop as a product of market forces rather than aggressive legislation, and should align its policy with the United States, France, and Great Britain to develop a joint network of key escrow authorities. Part I of this Note explains the operation of digital payment systems, digital money, and cryptography. Part I also sets forth existing legal safeguards against money laundering. Part II outlines the key escrow policies of the European Community, Great Britain, France, and the United States. Part III analyzes the European Commission's arguments against implementing key escrow and suggests that these arguments have been addressed and effectively rebutted by key escrow proposals in the United States and Great Britain. This Note concludes that a global network of key escrow authorities would provide law enforcement with the means to prevent digital money laundering.

NOTES

ENCRYPTED DIGITAL CASH TRANSFERS: WHY TRADITIONAL MONEY LAUNDERING CONTROLS MAY FAIL WITHOUT UNIFORM CRYPTOGRAPHY REGULATIONS

*Christopher D. Hoffman**

"We stand at the dawn of an age of global economic integration. Unfortunately, we are in some sense victims of our own progress."[1]

INTRODUCTION

Like the Trojan Horse, which hid a deadly enemy behind its deceptive charm, electronic payment systems[2] provide benefits

* J.D. Candidate, 1999, Fordham University. This Note is dedicated to the memory of my parents.

[1] *See Noble Warns of Technological Progress As Boon to Laundering*, 6 MONEY LAUNDERING ALERT 9 (1995) (quoting Ronald K. Noble, United States Undersecretary of the Treasury for Enforcement).

[2] *See* Laurie Law et al., *How to Make a Mint: The Cryptography of Anonymous Electronic Cash*, 46 AM. U. L. REV. 1131 (1997) (giving examples of electronic payment systems, including digital checks, credit cards, debit cards, and stored value cards); Catherine Lee Wilson, *Banking on the Net: Extending Bank Regulation to Electronic Money and Beyond*, 30 CREIGHTON L. REV. 671 (1997) (describing electronic checks as paper checks that are created and cleared electronically). A stored value card, also known as a "smart card" or "SVC" is

> a wallet-size card, similar in appearance to a credit card, with a magnetic strip or microprocessor embedded in the card. Value is loaded on the card by the issuer based on the amount of cash tendered by the customer. The card may be used to purchase goods or services. Value is removed from the card by the merchant providing goods or services.

Id. See also Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the Central Banks of the Group of Ten Countries, Security of Electronic Money at 30 (1996) [hereinafter Basle Report on Payment and Settlement Systems] (describing SVC as electronic purse). The term electronic purse, commonly used to refer to SVCs, is defined as:

> an IC card containing an application that stores a record of funds available to be spent or otherwise used by the holder; the record of funds is updated as transactions are made. Additional funds may be added to the stored balance through a withdrawal from a bank account or by other means. Sometimes referred to as a stored value card.

Id. The Basle Committee is,

> [a] Committee of banking supervisory authorities which was established by the

to consumers[3] while enabling money launderers to ply their trade with greater ease.[4] Consumers using digital payment systems can transfer money in its digital form[5] quickly and anony-

> central-bank Governors of the Group of Ten countries in 1975. It consists of senior representatives of bank supervisory authorities and central banks from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, Netherlands, Sweden, Switzerland, United Kingdom, and the United States. It usually meets at the Bank for International Settlements in Basle, where its permanent Secretariat is located.

Basle Committee on Banking Supervision, Core Principles for Effective Banking Supervision, at n.1 (1997) [hereinafter Basle Core Principles for Banking Supervision] The Committee on Payment and Settlement Systems established the Task Force on Security of Electronic Money which,

> [p]rimarily examined consumer-oriented stored-value payment products, a few of which have already been launched in large-scale pilot programmes in various countries; others are expected to be widely introduced in 1996 or 1997. Through interviews with suppliers, the Task Force identified general models of electronic money products and specific characteristics that are relevant to security. The Task Force found that the logical design chosen for the stored electronic "value", as well as the conditions under which such money balances can be transferred to other users, provide the basic framework for examining security measures in the various stored-value products . . . . The Task Force found that various security measures have been developed to protect the integrity, authenticity, and confidentiality of critical data and processes of electronic money products[, and that c]ryptography is the . . . critical safeguard for card-based systems and, indeed, the primary safeguard for software-based systems.

Basle Report on Payment and Settlement Systems, *supra*, at 1.

[3] *See* DANIEL C. LYNCH & LESLIE LUNDQUIST, DIGITAL MONEY, THE NEW ERA OF INTERNET COMMERCE 2-3 (1997) (noting benefits of digital payment systems such as inexpensive operation and easy access to greater selection of merchants from convenient location such as personal computer).

[4] *See* Financial Action Task Force, *1996-1997 Report on Money Laundering Typologies* ¶65 (visited Oct. 19, 1997) <http://www.oecd. org/fatf/fatfviii.htm#III.RECENT TRENDS AMONG FATF MEMBERS> (also on file with the *Fordham International Law Journal*) [hereinafter 1997 FATF Report] (describing concerns raised by potential criminal use of digital payment systems); Group of Ten, Report of the Working Party on Electronic Money, Electronic Money, Consumer Protection, Law Enforcement, Supervisory and Cross Border Issues (April 1997) [hereinafter Group of Ten Report on Electronic Money] (warning nations to closely monitor development of digital payment systems for criminal activity); *see also The Risks in Electronic Commerce*, INTELLIGENCE NEWSLETTER, Feb. 27, 1997 (identifying various factors enabling criminal use of electronic commerce including its anonymity, speed, and lack of legal oversight).

[5] *See* Lawrence H. White, *The Technology Revolution and Monetary Evolution*, *in* THE FUTURE OF MONEY IN THE INFORMATION AGE 15-16 (James A. Dorn, ed., 1997) (describing digital cash as spendable balance represented by string of digits in computer memory that constitutes claim on financial institution without being linked to any particular account); NATIONAL RESEARCH COUNCIL, COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 477 (Kenneth W. Dam and Herbert S. Lin, eds., 1996) [hereinafter "CRISIS REPORT"] (comparing digital cash to paper cash).

mously.[6] In addition, consumers can use cryptography,[7] a means to encode and decode messages with a numeric value called the key,[8] to secure electronic money transfers from theft and manipulation.[9] Having almost exclusive control of money transfers,[10] financial institutions have traditionally served as the safeguards against money laundering by maintaining records documenting the origin and destination of transferred funds.[11] Because digital payment systems do not require financial institutions to operate, individuals making digital payments can disregard regula-

> Digital cash is similar to paper cash in the sense that neither the paper on which paper money is printed nor the string of bits that represents digital cash has intrinsic value; value is conferred on a piece of paper or a particular string of bits if, and only if, an institution is willing to accept responsibility for them.

CRISIS Report, *supra*, at 477.

[6] *See* Law, *supra* note 2, at 1133 (describing operation of digital payment systems on computer networks); Basle Report on Payment and Settlement Systems, *supra* note 2, at 30 (describing how electronic wallets enable individuals to conduct transfers between SVCs and transfer money from bank account onto SVC via ATM machine or personal computer).

[7] *See* CRISIS REPORT, *supra* note 5, at 356 (defining cryptography as "the science and technology of keeping information secret from unauthorized parties by using a code . . . ."). Originally developed to protect military communications, cryptography has recently reached worldwide popularity as the means to secure Internet transactions and encode e-mail. LYNCH & LUNDQUIST, *supra* note 3, at 253.

[8] *See* CRISIS REPORT, *supra* note 5, at 376 (discussing operation of cryptography).

[9] *See* LYNCH & LUNDQUIST, *supra* note 3, at 70 (noting that use of cryptography in electronic transactions allows identification of parties, authentication of identities, nonrepudiation of the transaction, verification of data, and privacy).

[10] *See* ROBERT C. EFFROS, INTRODUCTION TO PAYMENT SYSTEMS OF THE WORLD xxvii-ix (Robert C. Effros, ed., 1994) (describing two types of money transfer system: debit transfer, where payee instructs his or her bank to collect from payor, and credit transfer, where payor instructs bank to debit payor's account and credit payee's account).

[11] *See* Bank Secrecy Act, 31 U.S.C. § 5313 (1994) (requiring financial institutions conducting transactions on behalf of single individual involving US$10,000 or more in aggregate to file Internal Revenue Service form 4789 Currency Transaction Report); Money Laundering Control Act, 31 U.S.C. § 5324 (1994) (criminalizing use of financial institutions to structure transactions to circumvent reporting requirements); 58 Fed. Reg. 46,014 (1993) (amending Bank Secrecy Act to impose reporting requirements on financial institutions conducting wire transfers); United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, U.N. Doc. E/CONF.82/15 (1988), *reprinted in* 28 I.L.M. 493 (1989) [hereinafter U.N. Convention Against Illicit Traffic or Convention] (mandating that signatory nations cooperate in producing financial institution records documenting suspect transactions); Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds From Crime, 30 I.L.M. 148 (1991) [hereinafter Council of Europe Convention] (requiring that signatory nations minimize negative effect of domestic bank secrecy laws on prosecution of money launderers); Council Directive No. 91/308, art. 3, O.J. L 166/77, at 79 (1991) [hereinafter Council Directive 91/308] (requiring financial institutions to keep records of customers conducting transactions involving 15,000 ECU or more).

tions that govern such institutions.[12] Without regulatory oversight and with the protection of cryptography, criminals can easily adapt digital payment systems for money laundering purposes.[13] In order to prevent this, law enforcement authorities must police digital money transfers.[14] A digital transfer encoded with cryptography will reveal nothing about its origin or destination.[15] Preventing digital money laundering therefore hinges on law enforcement's access to cryptographic keys.[16]

Recognizing the potential use of cryptography to hide criminal activity, the governments of Great Britain,[17] France,[18] and

[12] *See* Basle Report on Payment and Settlement Systems, *supra* note 2, at 35 (describing general model of payment system where users conduct transactions and transfers of money electronically without need for financial institutions to initiate transfers).

[13] *See* 1997 FATF Report, *supra* note 4, annex 1, ¶ 3 (describing difficulty of detecting money laundered using digital payment technology); Jeremy Platts, *Proliferating Cyberbanks Threaten Money Laundering Controls*, 8 MONEY LAUNDERING ALERT 8 (1997) (stressing that anonymity and easy transfer of digital money create law enforcement concerns); Sarah Jane Hughes, *"Cyberlaundering" Poses Threat to Controls*, 6 MONEY LAUNDERING ALERT 1 (1997) (noting that numerous daily transfers of assets enabled by digital payment systems will prevent effective containment of money laundering problem).

[14] *See* CRISIS REPORT, *supra* note 5, at 220 (stating that development of new telecommunications services will impose greater burden on law enforcement to intercept and decrypt suspect transmissions).

[15] *See* Jason Kerben, *The Dilemma for Future Communication Technologies: How to Constitutionally Dress the Crypto-Genie*, 5 COMMLAW CONSPECTUS 125, 129 (1997) (noting recent study finding that, in order to decrypt message encoded with 1,024 bit key, one would need one hundred computers with eight megabytes of memory operating at one hundred MHz for 280,000 years); Loring Wirbel *Big Bellcore Team Cracks RSA Code*, ELECTRONIC ENGINEERING TIMES, May 2, 1994, at 1 (stating that "[e]very 10-decimal digit equals approximately 33 bits"); *See* CRISIS REPORT, *supra* note 5, at 388 (stating that an attacker must attempt 2^{56} numeric combinations in order to find fifty-six bit, seventeen digit, cryptographic key); Gary Taubes, *Small Army of Code-Breakers Conquers a 129-Digit Giant; Team of Scientists Factors 129-Digit number used in Cryptography; Includes Related Information*, 264 ASAP 5160 (May 6, 1994) (describing how one research team cracked 425 bit key in eight months).

[16] *See* William R. Spernow, *Cybercrooks on the Net: Why Traditional Law Enforcement Will Be Unable to Cope With Threats to the Electronic Commerce System*, *in* MONEY LAUNDERING, ASSET FORFEITURE AND INTERNATIONAL FINANCIAL CRIMES 14 (Fletcher N. Baldwin, Jr. & Robert J. Munro, eds., 1997) (stating that encryption represents primary reason for increasing failure of law enforcement to prosecute Internet crime); Scott Sultzer, *Money Laundering: The Scope of the Problem and Attempts to Combat It* 63 TENN. L. REV. 143, 196 (noting that Internet banks can expand money laundering activities with impunity if law enforcement officials have no access to encrypted data).

[17] *See* UK Department of Trade and Industry, *Public Consultation Paper on Detailed Proposals for Legislation, Licensing of Trusted Third Parties for the Provision of Encryption Services, March 1997* (visited Sept. 3, 1997) <http://dtiinfo1.dti.gov.uk/pubs/> (also on file with the *Fordham International Law Journal*) [hereinafter British DTI Public Consultation Paper or Consultation Paper] (setting forth proposal for key escrow agency network).

the United States[19] have embraced key escrow[20] as a possible solution. Key escrow agencies provide law enforcement with access to transmissions encoded with cryptography by keeping records of all cryptographic keys in use by the public and releasing them under judicial subpoena.[21] The Commission of the European Communities[22] ("European Commission") opposes key escrow,

[18] *See Law No. 96-659, 26.7.96*, art. 17 (1996) <http://www.telecom.gouv.fr/english/activ/telecom/nloi17.htm> (also on file with the *Fordham International Law Journal*) [hereinafter French Key Escrow Regulation] (setting forth proposed amendment to French Telecommunications Act of 1996, Law No. 90-1170, 29.12.90, establishing key escrow agencies).

[19] *See* Bruce W. McConnell & Edward J. Appel, *Interagency Working Group on Cryptography Policy, Draft Paper: Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure, May 20, 1996* (visited Sept. 3, 1997) <http://www.isse.gmu.edu/pfarrell/nist/kmi.html> (also on file with the *Fordham International Law Journal*) [hereinafter White Paper] (setting forth Clinton Administration's proposal to replace export controls on cryptography with key escrow); *Statement of the Vice President, Al Gore, Cong. Press Release, Oct. 1, 1996* (visited Sept. 3, 1997) <http://www.epic.org/ crypto/key_escrow/clipper4_statement.html> (also on file with the *Fordham International Law Journal*) [hereinafter Gore Speech] (proposing to relax export controls in return for industry cooperation in developing key escrow system).

[20] *See* CRISIS REPORT, *supra* note 5, at 359 (defining escrowed encryption as "an encryption system that enables exceptional access to encrypted data through special data recovery keys held by a third party.").

[21] *See id.* at 168 (stating that escrow not only provides law enforcement with access to cryptographic keys, but also provides user services such as recovery of lost or corrupted keys).

[22] Treaty establishing the European Community, Feb. 7, 1992, [1992] 1 C.M.L.R. 573 [hereinafter EC Treaty], *incorporating changes made by* Treaty on European Union, Feb. 7, 1992, O.J. C 224/1 (1992), [1992] 1 C.M.L.R. 719, 31 I.L.M. 247 [hereinafter TEU]. The TEU, *supra*, amended the Treaty Establishing the European Economic Community, Mar. 25, 1957, 298 U.N.T.S. 11, 1973 Gr. Brit. T.S. No. 1 (Cmd. 5179-II) [hereinafter EEC Treaty], *as amended by* Single European Act, O.J. L 169/1 (1987), [1987] 2 C.M.L.R. 741 [hereinafter SEA], *in* TREATISES ESTABLISHING THE EUROPEAN COMMUNITIES (EC Off'l Pub. Off. 1987); *See* GEORGE A. BERMANN ET AL., CASES AND MATERIALS ON EUROPEAN COMMUNITY LAW 57 (stating that European Commission functions as "[European] Community's executive organ"); EC Treaty, *supra*, arts. 155-63, [1992] 1 C.M.L.R. at 682-84 (setting forth powers of Commission). The powers of the European Commission, as set forth in Article 155 of the EC treaty, include:

> -ensur[ing] that the provisions of [the EC Treaty] and the measures taken by institutions persuant thereto are applied;
>
> -formulat[ing] recommendations or delivering opinions on matters dealt with in [the EC Treaty], if it expressly so provides or if the Commission considers is necessary;
>
> -hav[ing] its own power of decision and participat[ing] in the shaping of measures taken by the Council and by the European Parliament in the manner provided for in [the EC Treaty];
>
> -exercis[ing] the powers conferred on it by the Council for the implementation of the rules laid down by the latter.

Id., art 155, [1992] 1 C.M.L.R. at 682. *See* DERRICK WYATT & ALAN DASHWOOD, EUROconsidering it an unnecessary burden on commerce that is better left to the scrutiny of the market.[23] Proponents of key escrow respond by arguing that economic expediency should not trump the interests of law enforcement, and that a coordinated multinational effort to create a network of key escrow agencies would prevent the use of cryptography for criminal purposes.[24]

This Note argues that key escrow represents a solution to the problem of digital money laundering. In addition, this Note argues that the European Commission has wrongly concluded that key escrow should develop as a product of market forces rather than aggressive legislation, and should align its policy with the United States, France, and Great Britain to develop a joint network of key escrow authorities. Part I of this Note explains the operation of digital payment systems, digital money, and

PEAN COMMUNITY LAW 665 (3d ed. 1993) (stating that term "European Union" refers to political relationship between three pillars of European Community). The Treaty on European Union created a single Union comprised of three Communities: the European Economic Community ("EEC"), the European Coal and Steel Community ("ECSC"), and the European Atomic Energy Community ("Euratom"). Treaty on European Union, Feb. 7, 1992, O.J. C 224/1 91992), [1992] 1 C.M.L.R. 719, 31 I.L.M. 247 [hereinafter TEU] *amending* Treaty Establishing the European Economic Community, Mar. 25, 1957, 298 U.N.T.S. 11, 1973 Gr. Brit. T.S. No. 1 (Cmd. 5179-II) [hereinafter EEC Treaty], *as amended by* Single European Act, O.J. L 169/1 (1987), [1987] 2 C.M.L.R. 741 [hereinafter SEA], *in* TREATIES ESTABLISHING THE EUROPEAN COMMUNITIES (EC Off'l Pub. Off. 1987)). The EEC, ECSC, and Euratom comprise the first of three pillars that form the European Union. WYATT & DASHWOOD, *supra*, at 655. Identified by the TEU, the second and third pillars are the Provisions on a Common Foreign and Security Policy and Provisions on Co-operation in the Fields of Justice and Home Affairs. TEU, *supra*, tits. V, VI, O.J. C 224/1, at 94-97 (1992), [1992] 1 C.M.L.R. at 729-35. Fifteen Member States comprise the European Union today. OFFICE FOR OFFICIAL PUBLICATIONS OF THE EUROPEAN COMMUNITIES, BUILDING EUROPE TOGETHER 15 (1997). The Member States include Germany, France, Italy, the United Kingdom, Ireland, Denmark, Belgium, Luxembourg, the Netherlands, Greece, Spain, Portugal, Sweden, Finland, and Austria. *Id.* The European Union has also committed itself to officially discuss the future membership of Hungary, Poland, Romania, Slovakia, Latvia, Estonia, Lithuania, Bulgaria, Czech Republic, and Slovenia. *Id.*

[23] *See* Commission of the European Communities, Ensuring Security and Trust in Electronic Communication: Towards a European Framework for Digital Signatures and Encryption: Communication from the Commission to the European Council, European Parliament, and the Committee of the Regions COM (97) 503 Final at 12 [hereinafter Communication on European Encryption Policy] (suggesting that market forces should determine propriety of key escrow and stating that imposition of key escrow "could lead to market obstacles and reduce the competitiveness of the European industry.").

[24] *See* British DTI Public Consultation Paper, *supra* note 17, ¶ 18 (stressing need for key escrow network international in scope); CRISIS REPORT, *supra* note 5, at 11 (suggesting that U.S. government work with other nations to maximize benefit of key escrow).

cryptography. Part I also sets forth existing legal safeguards against money laundering. Part II outlines the key escrow policies of the European Community, Great Britain, France, and the United States. Part III analyzes the European Commission's arguments against implementing key escrow and suggests that these arguments have been addressed and effectively rebutted by key escrow proposals in the United States and Great Britain. This Note concludes that a global network of key escrow authorities would provide law enforcement with the means to prevent digital money laundering.

I. *ELECTRONIC MONEY AND MONEY LAUNDERING*

Unlike traditional wire transfer systems that employ financial institutions, digital payment systems enable individuals to transfer money or conduct Internet transactions[25] on a personal computer.[26] Commentators point out that digital money secured by cryptography enhances the utility of the Internet and drives the expansion of electronic commerce.[27] Experts estimate that more than 200 million people will use the Internet regularly by the year 2000,[28] and that electronic commerce will amount to more than three trillion U.S. dollars by the year 2005.[29] This prospective increase in electronic trade has forced

[25] *See* LYNCH & LUNDQUIST, *supra* note 3, at 15 (noting that, today, consumers pay for goods and services purchased on Internet primarily with credit cards).

[26] *See* Rosalind L. Fisher, *New Payments Technology*, *in* THE FUTURE OF MONEY IN THE INFORMATION AGE 60-61 (James A. Dorn, ed., 1997) (describing electronic payment system called Visa Interactive maintained by Visa and its member banks that allows customers to conduct transactions using interactive television, home computer, or touch tone telephone).

[27] *See* LYNCH & LUNDQUIST, *supra* note 3, at 2 (noting that "a new world order is arising in mechanisms for value exchange among human beings[, d]igital money is the cuneiform of a new age.").

[28] *See* Wilson, *supra* note 2, at 673 (noting that today more than thirty million people worldwide use Internet, and over thirty-five million households in United States have personal computers).

[29] *Id.* In 1994, Internet purchases were estimated at US$240 million. John Kavanagh, *Purchases on the Internet Could Potentially Exceed $200bn by Year 2000*, FIN. TIMES, Nov. 1, 1995, at 12 FT-IT. The Internet can support entire shopping malls, offering everything from detailed product specifications to recorded sales pitches. A. Michael Froomkin, *Regulation and Computing and Information Technology: Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, 15 J. L. & COMM. 395, 450 (1997). Notably, the Clinton Administration's Framework for Global Electronic Commerce stresses that,

> [n]o single force embodies our electronic transformation more than the evolving medium known as the Internet. One a tool reserved for scientific and

law enforcement officials to focus on the possible use of electronic payment systems for money laundering.[30]

Criminals launder money using financial institutions and businesses that serve to associate the funds with legitimate sources.[31] Law enforcement authorities detect money laundering by policing financial institutions that transfer money.[32] Some commentators suggest that, because digital payment systems operate independently of financial institutions, law enforcement authorities should also police electronic transmissions.[33] One way to perform this task lies in the creation of key escrow agencies[34] that would maintain copies of cryptographic

> academic exchange, the Internet has emerged as an appliance of every day life, accessible from almost every point on the planet. . . . The Internet is being used to reinvent government and reshape our lives and our communities in the process. . . . New models of commercial interaction are developing as businesses and consumers participate in the electronic marketplace and reap the resultant benefits.

President William J. Clinton and Vice President Albert Gore Jr., Framework for Global Electronic Commerce (July 1, 1997), at 1 (visited October 3, 1997) <http://www.whitehouse.gov/WH/New/Commerce/> (also on file with the *Fordham International Law Journal*) [hereinafter Framework for Global Electronic Commerce]. The Commission of the European Communities similarly notes that "[i]t is estimated that electronic commerce revenues, both direct and indirect, on the Internet may increase to over 2 billion ECU worldwide by the year 2000." Commission of the European Communities, A European Initiative in Electronic Commerce: Communication from the Commission to the European Parliament, the Economic and Social Committee, and the Committee of the Regions, COM (97) 157 Final (April 1997), at 4, ¶ 4 [hereinafter European Initiative in Electronic Commerce].

[30] *See* Graeme Browning, *Cybercops and Robbers*, 29 NAT. J. 590 (1997) (stating that "[l]aw enforcement officials skilled in the emerging field of cybercrime believe the development of E-cash means that extortion, racketeering and money laundering will become virtually impossible to detect and stop.").

[31] *See generally* Sultzer, *supra* note 16, at 148-51 (discussing mechanics of money laundering, including "placement," "layering," and "integration").

[32] *See id.* at 151-84 (discussing money laundering legislation in United States mandating financial institutions to maintain reports and records to facilitate investigations or legal proceedings).

[33] *See, e.g.*, Peter Nielsen, *G10 Mulls Effect of E-Cash on Policy and Fraud*, REUTER EUR. BUS. REP., July 4, 1996 (stating that "[o]ne of the concerns of central bankers is that some smart card systems do not leave an audit trail and allow for the direct transfer of money . . . [a]nonymous transactions raise the possibility of money laundering and illegal activities as criminals transfer money between cards across borders instead of using suitcases"); CRISIS REPORT, *supra* note 5, at 90-94 (arguing that encrypted electronic transmissions will frustrate investigative efforts unless law enforcement authorities have access to their content).

[34] *See* CRISIS REPORT, *supra* note 5, at 167-68 (defining escrowed cryptography as system that allows access to encrypted messages by establishing agencies called trusted third parties to hold copies of all cryptographic keys in use by public).

keys.[35] Because encryption represents the primary means to secure electronic transmissions, proponents of key escrow stress that legal authorities must have access to cryptographic keys[36] in order to conduct timely investigations.[37]

A. *Electronic Money*

As early as 1200 AD, Italian merchants made payments by adding and subtracting figures on bank balance sheets without exchanging physical currency.[38] Today, balance sheet entries exist as data in computer memory.[39] Electronic money encompasses both digital representation[40] of legal tender and electronic coins[41] accepted by merchants on the Internet.[42] Called the cornerstone of digital money,[43] cryptography prevents forgery and verifies the identity of parties to deter repudiation of electronic transactions.[44]

[35] *See id.* 170 (warning that failure to implement some form of key escrow may result in "proliferation of products with encryption capabilities that would seriously weaken, if not wholly negate, the authority to wiretap . . . and damage intelligence collection for national security and foreign policy reasons.").

[36] *See* LYNCH & LUNDQUIST, *supra* note 3, at 68 (defining cryptographic key as "a set of rules for substituting one character for another.").

[37] CRISIS REPORT, *supra* note 5, at 91. FBI Director Louis Freeh has warned that "unless the issue of encryption is resolved soon, criminal conversations over the telephone and other communications devices will become incipherable by law enforcement [and] this, as much as any issue, jeopardizes the public safety and national security of [the United States]." *Id.*

[38] *See* White, *supra* note 5, at 15-16 (discussing evolution of electronic fund transfer systems).

[39] *Id.*

[40] *See* Federal Deposit Insurance Corporation, General Counsel's Opinion No. 8, Stored Value Cards, 61 Fed. Reg. 40490 (1996) [hereinafter FDIC General Counsel's Opinion No. 8] (setting forth conditions under which electronic funds underlying balance on stored value card represent deposit for purposes of deposit insurance coverage); *see also* White, *supra* note 5, at 16 (stating that "currency balance information, an encoded string of digits, can be carried on a 'smart' plastic card with an implanted microchip, or carried on a computer hard drive").

[41] *See* Froomkin, *supra* note 29, at 458 (describing digital coin as unit of value identified by encrypted serial number in computer memory).

[42] JONATHAN R. MACEY & GEOFFREY P. MILLER, BANKING LAW AND REGULATION 41 (1997); *see* LYNCH & LUNDQUIST, *supra* note 3, at 23-40 (describing various vendors of digital money, including Checkfree, CyberCash, DigiCash and First Virtual).

[43] *See* White, *supra* note 5, at 15-16 (defining digital money as spendable balance represented by computer data constituting claim on financial institution without being linked to any particular account).

[44] *See* LYNCH & LUNDQUIST, *supra* note 3, at 67 (explaining that encryption constitutes cornerstone in security and creation of digital money).

1. Conventional Money Distinguished

Traditional fiat currency[45] transferred physically or by wire[46] comprises the best known payment system.[47] Traditionally issued and regulated by banks, money is often influenced by forces shaping the banking industry.[48] As modern banks make greater use of electronic fund transfer systems and expand operations into cyberspace,[49] money evolves into electronic forms such as the electronic coin[50] and value stored on a Stored Value

[45] *See* JOHN MAYNARD KEYNES, A TREATISE ON MONEY 11 (1930) (defining fiat money as money that only represents objective standard that comprises its value).

[46] *See* Effros, *supra* note 10, at xxvii-ix (stating that wire transfer systems include debit transfer, where payee instructs his or her bank to collect payor, and credit transfer, where payor instructs bank to debit payor's account and credit payee's account).

[47] Henry H. Perritt, Jr., *Legal and Technological Infrastructures for Electronic Payment Systems*, 22 RUTGERS COMPUTER & TECH. L.J. 1, 4 (1996).

[48] *See id.* at 15-20 (explaining development of money in context of banking).

[49] *See* Wilson, *supra* note 2, at 19 (noting that emergence of Internet bank evidences tremendous consumer appeal of electronic banking). Security First Network Bank ("SFNB"), the first of two national banks to operate almost exclusively on the Internet, opened on October 18, 1995. *Id.* Located at <http://www.sfnb.com>, SFNB offers various types of deposit account services, including checking and savings accounts, money market funds, certificates of deposit, an ATM/debit card, and a credit card. *Id.* A 1996 report indicates that SFNB has attracted over 8000 customers and amassed Over US$41 million in assets. Mickey Meece, *Internet Bank's Offering of a Credit Card Proves a Hit with Its Customers*, AM. BANKER, Dec. 16, 1996, at 18. The second Internet Bank, Atlanta Internet Bank, opened in October of 1996. Jennifer Kingson Bloom, *A Second Bank is Launched into Cyberspace*, AM. BANKER, Oct 18, 1996 at 1. Located at <http://www.atlantabank.com>, it is currently a part of Carolina First Corp., a bank with US$1.5 billion in assets. Wilson, *supra* note 2, at 677. Atlanta Internet Bank currently offers only money market, savings and checking accounts, electronic bill payment services, and ATM cards, but plans to offer loan products and brokerage services by the end of 1997. *Id.* In addition to Atlanta Internet Bank and SFNB, one study has indicated that at least 500 other banks maintain cites on the Internet. Thomas P. Vartanian, *Many Evolutionary Factors Point One Way: The Internet*, AM. BANKER, Dec. 23, 1996, at 4A.

[50] *See* Brian W. Smith & Ramsey J. Wilson, *The Electronic Future of Cash: How Best to Guide the Evolution of Electronic Currency Law*, 46 AM. U. L. REV. 1105, 1109 (1997) (noting that distinction between traditional legal tender and electronic value takes on particular importance in determining whether issuers of electronic coins usurp government's exclusive right to coin money). For example, under the Stamp Payments Act of 1862, 18 U.S.C. § 336 (1994), only the government can issue money in denominations of less than one dollar. Commentators point out that the Act's legislative history reveals congressional intent to prevent inflation caused by a shortage of government-issued coins, and that electronic payment systems involve the transfer rather than issuance of money. *Id.* at n.27. Because digital coins must be redeemed for their underlying value, they resemble commercial paper rather than legal tender. *See id.* at 1111 (noting that existence of multi-purpose check payment systems since 1891 and fact that digital money digital money resembles checks indicates that issuers of digital coins do not encroach on the government's exclusive right to coin money).

Card ("SVC").[51]

a. Regulated Electronic Fund Transfers

Individuals can transfer money using a personal computer programmed with home banking software,[52] an automated teller machine,[53] or a financial institution providing wire transfer services.[54] Article 4A of the U.S. Uniform Commercial Code[55] sets forth rules governing wholesale electronic funds transfers.[56] The United Nations[57] Commission on International Trade ("UNCITRAL")[58] looked to Article 4A in drafting its Model Law on International Credit Transfers.[59] Unlike Article 4A, which covers money transfers in the United States, the UNCITRAL Model Law was drafted to primarily govern international trans-

[51] *See generally* LYNCH & LUNDQUIST, *supra* note 3, at 23-60 (describing various electronic payment systems such as Checkfree, CyberCash, DigiCash, First Virtual Holdings, and NetBill); Wilson, *supra* note 2, at 671 (describing operation of Stored Value Cards ("SVC")).

[52] *See* Tom Foremski, *Web Browsers Beat Brick and Mortar*, FIN. TIMES, Sept. 4, 1996, at 4 (discussing recent shift in consumer preference from personal teller service at local branch to home banking via personal computer).

[53] *See* 12 C.F.R. § 229.2(c) (defining automated teller machine or ATM as "an electronic device at which a natural person may make deposits to an account by cash or check and perform other account transactions").

[54] Basle Report on Payment and Settlement Systems, *supra* note 2, at 3.

[55] *See* Richard L. Field, *The Electronic Future of Cash: Survey: 1996: Survey of the Year's Developments in Electronic Cash Law and the Laws Affecting Electronic Banking in the United States*, 46 AM. U.L. REV. 967, 973 (1997) (stating that forty-nine states adopted Uniform Commercial Code by 1996).

[56] U.C.C. § 4A-102 (1996). Regarding the scope of Article 4A, the official comment to section 4A-104 states that

> Article 4A governs a method of payment in which the person making the payment (the "originator") directly transmits an instruction to a bank either to make payment to the person receiving payment (the "beneficiary") or to instruct some other bank to make payment to the beneficiary. The payment from the originator to the beneficiary occurs when the bank that is to pay the beneficiary becomes obligated to pay the beneficiary.

Id. § 4A-104 (official comment). Article 4A does not apply to consumer transactions covered under federal law. *Id.* § 4A-108.

[57] *See* U.N. CHARTER art. 1(1), 1(2) (describing United Nations as international organization of fifty states formed to "develop friendly relations among nations," and "to maintain international peace and security . . . ."). The United Nations was formed with the signing of the U.N. Charter in San Francisco in April of 1945. PETER R. BAEHR & LEON GORDENKER, THE UNITED NATIONS IN THE 1990s 1-3 (2nd ed. 1994).

[58] *See* Eric E. Bergsen, *A Payment Law for the World: UNCITRAL Model Law on International Credit Transfers*, *in* PAYMENT SYSTEMS OF THE WORLD 409 (Robert C. Effros, ed., 1994) (noting that UNCITRAL's first session in 1968 included discussion of international payments).

[59] *Id.* at 416.

fers.[60] In addition, the UNCITRAL Model Law contains various customer protection rules which, in the United States, are found in the Electronic Fund Transfer Act of 1978.[61] In the United States, the 1978 Electronic Fund Transfer Act[62] sets forth the rights of consumers using electronic fund transfer systems.[63] The Act is implemented by the Federal Reserve Board's[64] Regulation E.[65] Regulation E requires financial institutions offering electronic fund transfer[66] services to make various disclosures to customers[67] and to furnish a receipt after the customer initiates a transfer.[68] Regulation E also limits customers' liability for unauthorized transfers[69], provides for error resolution procedures,[70] and restricts circumstances under which the institution can authorize access to a customer's account.[71]

Current trends foreshadow a fundamental shift in banking from personal service to electronic media.[72] One study predicts

[60] *Id.* at 417.

[61] *Id.* at 417 n.31.

[62] 15 U.S.C. §§ 1693-1693(r) (1994). The Electronic Fund Transfer Act defines electronic fund transfer as "any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account." *Id.* § 1693(a)(6).

[63] *See* Effros, *supra* note 10, at xxxi (discussing purpose and provisions of Electronic Fund Transfer Act of 1978).

[64] *See* MACEY & MILLER, *supra* note 42, at 66-67 (describing U.S. Federal Reserve System). Comprised of twelve Federal Reserve Banks and a seven member board of governors, the U.S. Federal Reserve System exercises broad control over the monetary supply and regulates bank holding companies and member banks in the Federal Reserve System. *Id.*

[65] Electronic Fund Transfers (Regulation E), 12 C.F.R. § 205.

[66] *See id.* § 205.3(b) (defining electronic fund transfer as "any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for purpose of ordering, instructing, or authorizing a financial institution to debit or credit an account.").

[67] *Id.* § 205.7(b). Regulation E requires financial institutions to disclose the extent of the customer's liability for unauthorized electronic transfers and information about fees, procedure to stop payment and the financial institution's liability for failure to comply with a stop order, confidentiality of the customer's account information, and error resolution procedures. *Id.*

[68] *Id.* § 205.9(a).

[69] *Id.* § 205.6(b).

[70] *Id.* § 205.11(b). The customer initiates the error resolution procedures by giving oral or written notice to the financial institution no later than 60 days after the institution sends the statement on which the alleged error first appears. *Id.*

[71] *Id.* § 205.5(a).

[72] *See, e.g.,* Debt Collection and Improvement Act of 1996, Pub. L. No. 104-134, 110 Stat. 1321-374 (mandating that all federal agencies make electronic payments to

that home banking in the United States will increase from about 700,000 users in 1995 to more than five million, or seventy-five percent of all U.S. homes, by the year 2000.[73] Recognizing the significance of such statistics, banks increasingly seek to form alliances with software and computer firms.[74] With a ten-to-one cost ratio of accepting an over-the-counter deposit versus a direct deposit, many banks look to electronic transactions as a means to reduce costs.[75] Industry analysts have noted that banks which fail to recognize the importance of alternative delivery systems may suffer significant competitive detriment.[76]

b. Wire Transfer Systems

Traditional payment systems facilitate money transfers using a network of government-regulated financial institutions.[77] Electronic transfer systems[78] in the United States include the Federal Reserve Wire Network[79] ("FedWire"), Clearing House Interbank Payment System[80] ("CHIPS"), and the Society for Worldwide In-

individuals who apply for "federal benefit programs, begin employment with a federal agency, apply for retirement benefits, enter into a contract or purchase order with the federal government or file or renew a grant application" beginning in January, 1999). The Department of Treasury is currently considering a proposal to implement this law by issuing federal benefits on SVCs. Wilson, *supra* note 2, at 687.

[73] *See* Foremski, *supra* note 52, at 4 (citing recent study conducted by U.S. marketing firm Jupiter Communications).

[74] *See id.* (noting that Microsoft chairman Bill Gates predicted that "every bank will choose to have its own Internet presence.").

[75] *See* White, *supra* note 5, at 19 (noting that electronic fund transfers "lower the cost of wiring money from $20 to 2 cents or less per transaction.").

[76] *See id.* (stating that "[j]ust as the dinosaurs either evolved into different animals or became extinct, banks will either quickly evolve into new organizations or become extinct [and the] test for banks' adaptability will be what they do with their branch networks."); *see also* Judge W. Fowler, *The Branch is Dead!*, A.B.A. BANKING J., Apr., 1995, at 40 (stating that "[i]f you turned every branch into a 7-11 store, the revenues generated would be in excess of ten times those generated by a typical bank branch.").

[77] Bruce J. Summers, *The Payment System in a Market Economy*, *in* THE PAYMENT SYSTEM: DESIGN, MANAGEMENT AND SUPERVISION 3-4 (Bruce J. Summers, ed., 1994).

[78] *See* Fletcher N. Baldwin, Jr., *Money Laundering and Wire Transfers: When the New Regulations Take Effect Will They Help?*, 14 DICK. J. INT'L L. 413, 422 (1996) (noting that 110 million wire transfers in 1995 moved around US$474 trillion).

[79] *See* Effros, *supra* note 10, at xxxii (noting that rules governing FedWire transfers are set forth in Subpart B of the Federal Reserve's Regulation J, 12 C.F.R. § 210).

[80] *See id.* (describing Clearing House Interbank Payment System ("CHIPS") as communications network and clearing facility that handles domestic and international funds transfers).

terbank Financial Telecommunication ("SWIFT") system.[81] Operated by the twelve U.S. Federal Reserve Banks,[82] FedWire connects U.S. government agencies, Federal Reserve member banking institutions and their customers, and the Federal Reserve Banks.[83] CHIPS functions as the United States' primary international electronic funds transfer system.[84] It is comprised of 140 international and domestic financial institutions.[85] The Comptroller of the Currency,[86] the Federal Reserve System, and the Federal Deposit Insurance Corporation[87] regulate CHIPS.[88] SWIFT mainly functions as an international communications system, facilitating FedWire and CHIPS transfers by transmitting financial information such as payment instructions and statements.[89]

Electronic payment systems in other countries include the French SAGITTAIRE,[90] the Italian SETIF,[91] the Japanese

[81] *See* Baldwin, *supra* note 78, at 424 (noting that Society for Worldwide Interbank Financial Telecommunication ("SWIFT") also works in conjunction with FedWire and CHIPS systems). SWIFT is owned and operated by the Society for Worldwide Interbank Financial Telecommunications S.C., a Belgian cooperative society comprised of 1500 international financial institutions. Baldwin, *supra* note 78, at 423.

[82] *See* MACEY & MILLER, *supra* note 42, at 66-67 (stating that Federal Reserve, comprised of 12 Federal Reserve Banks and seven-member board of governors, controls money supply and oversees U.S. bank holding companies and Federal Reserve member banks).

[83] Baldwin, *supra* note 78, at 422.

[84] Effros, *supra* note 10, at xxxii. *See* Baldwin, *supra* note 78, at 423 (noting that CHIPS transfers in 1990 amounted to approximately US$222 trillion).

[85] Baldwin, *supra* note 78, at 423.

[86] *See* MACEY & MILLER, *supra* note 42, at 67 (describing Comptroller of the Currency). Housed within the Department of the Treasury, the Office of the Comptroller of the Currency charters and supervises national banks. *Id.*

[87] *See id.* (describing Federal Deposit Insurance Corporation). The Federal Deposit Insurance Corporation ("FDIC") provides federal deposit insurance to national banks, state-chartered commercial banks, thrifts, savings banks, and savings and loans. *Id.* The FDIC also retains regulatory authority over the banks which it insures and acts as receiver in the event of their failure. *Id.* at 68.

[88] Baldwin, *supra* note 78, at 423.

[89] *Id.* at 424; *see* Samuel Newman, *Society for Worldwide Interbank Financial Telecommunication (SWIFT), in* PAYMENT SYSTEMS OF THE WORLD 381 (Robert C. Effros, ed., 1994) (noting that SWIFT grew from fifteen member countries and 239 banks in 1973 to ninety-six member countries and 3903 banks in 1992).

[90] Michael Perdrix, *France, in* PAYMENT SYSTEMS OF THE WORLD 148, 155 (Robert C. Effros ed., 1994). The acronym SAGITTAIRE stands for "Système Automatique de Gestion Intègrèe par Tèlètransmission de Transactions avec Imputation de Règlemens 'Etranger.'" *Id.*

[91] Lucio Cerenza, *Italy, in* PAYMENT SYSTEMS OF THE WORLD 201 (Robert C. Ef-

Gaitame-yen,[92] the British CHAPS,[93] and the Swiss SIC[94] systems. The SAGITTAIRE system exclusively controls international transfers of French francs.[95] In 1990, SAGITTAIRE processed 2,448,060 electronic messages representing 35,393 billion francs.[96] SETIF was created in 1980 to streamline and organize the Italian interbank funds transfer system.[97] The Foreign Exchange Yen Settlement System, or Gaitame-yen has been described as the Japanese version of CHIPS.[98] The system settles yen transfers arising from international payments and foreign exchange transactions.[99] CHAPS, an acronym for the Clearing House Automated Payment System, provides same-day credit transfers and settlement for payments of 5,000 British pounds and above.[100] Rather than use a central disbursement facility, each CHAPS member uses a personal computer called the CHAPS Gateway to send and receive payment messages.[101] SIC, or Swiss Interbank Clearing, handles interbank payments between Swiss banks.[102] The volume of SIC payments on an average day in 1992 totaled approximately 131 billion Swiss francs and 253,000 interbank payments.[103]

2. Digital Money

Economic success of SVCs and digital coins will be determined to a great extent by industry, governments, regulatory agencies, and consumers.[104] Industry, comprised of multina-

fros ed., 1994). The Acronym SETIF stands for "Servizio elettronico di transferimento inerbancario di fondi." *Id.*

[92] Eikichi Saito, *Japan*, in PAYMENT SYSTEMS OF THE WORLD 222 (Robert C. Effros ed., 1994).

[93] Anthony Beaves, *United Kingdom, in* PAYMENT SYSTEMS OF THE WORLD 356 (Robert C. Effros, ed., 1994).

[94] Martin Hess, *Switzerland, in* PAYMENT SYSTEMS OF THE WORLD 318 (Robert C. Effros ed., 1994).

[95] Perdrix, *supra* note 90, at 148.

[96] *Id.*

[97] Cerenza, *supra* note 91, at 201.

[98] Saito, *supra* note 92, at 222.

[99] *Id.* at 223.

[100] Beaves, *supra* note 93.

[101] *Id.* at 357.

[102] Hess, *supra* note 94, at 316.

[103] *Id.* at 318.

[104] Felix Stalder, *Electronic Money: Preparing the Stage*, at 8, 9. (visited Sept. 1, 1997) <http.www.fis.utoronto.ca /~stalder/html/e-cash1.html#Electronic> (also on file with the *Fordham International Law Journal*).

tional banking corporations and computer manufacturers, plays a key role in the development digital payment systems by generating an infrastructure to support digital cash transactions.[105] Governments[106] and regulatory agencies determine the legal environment in which electronic money systems will operate.[107] The users of electronic money, both customers and merchants, influence its technical character indirectly by choosing one payment system over another.[108]

a. Stored Value Cards

SVCs, also known as smart cards, hold a prepaid amount of funds that consumers can access by inserting the card into a de-

[105] *Id.* at 8.

[106] *See e.g.,* William J. Clinton, *Office of the Press Secretary, Presidential Directive, Memorandum for the Heads of Executive Departments and Agencies, (July 1, 1997)* (visited Oct. 3,1997) <http://www. whitehouse.gov/WH/New/Commerce/> (also on file with the *Fordham International Law Journal*) [hereinafter Clinton Administration Directive] (articulating Clinton Administration's policy on electronic commerce). On July 1, 1997, the Clinton Administration issued a Presidential Directive entitled Memorandum for the Heads of Executive Departments and Agencies. In the Presidential Directive, President Clinton urges the United States to cooperate with non-U.S. governments and the private sector to facilitate the development of electronic payment systems:

> I direct the U.S. Trade Representative to work with foreign governments to monitor newly developing experiments in electronic payment systems; to oppose attempts by governments to establish inflexible and highly prescriptive regulations and rules that might inhibit the development of new systems for electronic payment; and as electronic payment systems develop, to work closely with the private sector in order to keep apprised about policy development and ensure that governmental activities flexibly accommodate the needs of the emerging marketplace.

Id. The Commission of the European Communities expressed similar sentiments:

> The aim of this initiative is to encourage the vigorous growth of electronic commerce in Europe.
>
> . . .
>
> Foster a favourable business environment for electronic commerce by promoting adequate skills, and by making consumers and industry aware of the opportunities offered by electronic commerce. This will be realized through training, information and demonstration projects; by exploiting synergies between government and industries . . . .
>
> Work towards global consensus from a common European position to ensure effective participation in current international cooperation and negotiations . . . .

European Initiative In Electronic Commerce, *supra* note 29, COM (97) 157 Final, at 1-2, ¶¶ 1-4.

[107] Stalder, *supra* note 104, at 8.

[108] *Id.*

vice called the point of sale terminal.[109] Merchants can transfer the funds accumulated at the terminal to a bank account by telephone.[110] One type of stored value card, the magnetic-stripe card,[111] can be used at terminals mounted on photocopiers or laundry machines.[112] Commuters in New York, San Francisco, and Washington D.C. can use magnetic-stripe cards to pay mass transit fares.[113] In Europe, the cards are adopted for use at public telephones.[114] Unlike magnetic-stripe cards, SVCs contain a microprocessor chip which stores and computes funds.[115] Individuals can download money from a bank account directly onto the SVC and transfer the proceeds to other SVCs using an electronic wallet, a device similar to a point of sale terminal adopted for use in person-to-person SVC transfers.[116] Already introduced in Europe and Asia, electronic wallets that operate on computer hard drives allow individuals to transfer money via modem anywhere in the world.[117]

Stored value cards can be implemented in a number of different ways[118] which generally differ in the treatment of funds underlying the electronic value on the SVC chip.[119] The U.S.

[109] Walter A. Effross, *Putting the Cards Before the Purse? Distinctions, Differences, and Dilemmas in the Regulation of Stored Value Card Systems*, 65 UMKC L. REV. 319, 323 (1997); *see* Mark E. Budnitz, *Stored Value Cards and the Consumer: The Need for Regulation* 46 AM. U.L. REV. 1027, 1031 (1997) (stating that SVCs look similar to ATM or credit cards because they are used in traditional ATM terminals).

[110] *Id.*

[111] *See* Smith & Wilson, *supra* note 50, at 1106 (stating that magnetic stripe cards provide limited read-only data in magnetic form).

[112] *See id.* (discussing versatility of SVCs).

[113] *See* Effros, *supra* note 109, at 326 (noting everyday use of SVCs).

[114] *Id.* at 326 n.26; *see also* Russel Mitchell, *The Smart Money is on Smart Cards*, BUS. WK., Aug 14, 1995 at 68 (noting that nearly 33 million smart cards were issued in Europe and Asia by end of 1995).

[115] Basle Report on Payment and Settlement Systems, *supra* note 2, at 6.

[116] *See id.* at 30 (defining electronic wallet as "a computer device used in some electronic money systems which can contain an IC card or in which IC cards can be inserted and which may perform more functions than an IC card."). The term electronic wallet could also encompass the smart card itself. Froomkin, *supra* note 29, at 465 (noting that "[a]n electronic wallet is a smart card with a microprocessor on it. The wallet interacts with specifically designed card readers, somewhat like bank cards are used in Automatic Teller Machines.").

[117] Effros, *supra* note 109, at 326 n.21. Law, *supra* note 2, at 1133.

[118] *See* Budnitz, *supra* note 109, at 1032 (warning that numerous ways of implementing SVCs could prevent consumers from making fully informed choices about which SVC systems to use and suggesting that regulators require SVC issuers to disclose pertinent information to eliminate any confusion).

[119] FDIC General Counsel's Opinion No. 8, *supra* note 40, at 40,490.

Federal Deposit Insurance Corporation separates stored value card systems into one of four types based on this distinction.[120] In addition to the distribution of funds underlying the electronic value, SVCs also differ in the degree of contact with a central clearing facility[121] present during the transaction.[122] In the sys-

[120] *Id.* In the Bank-Primary Customer Account System, funds underlying the SVC remain in the customer's account until a payee contacts the bank to make a claim. *Id.* at 40,493. This system operates similarly to a debit card, although funds are debited from a microchip embedded in the SVC rather than directly from the customer's account. *Id.* at 40,490. In the Bank Primary-Reserve Systems, value is downloaded onto a customer's SVC and the corresponding funds withdrawn from the customer's account and placed into a reserve account for eventual transfer to payees. *Id. See* Gary W. Lorenz, *Electronic Stored Value Payment Systems, Market Position and Regulatory Issues* 46 AM. U.L. REV. 1177, 1183 (1997) (warning that, because financial institutions have no way of ascertaining total amount of value outstanding on all SVCs, successful fraud that depletes funds in reserve account may not come to light until entire system becomes insolvent). In the Bank Secondary-Advance Systems, a third party creates electronic value and distributes it to depository institutions. FDIC General Counsel's Opinion No. 8., *supra* note 40, at 40,490. As customers obtain the electronic value, the depository institution pays the funds to the issuer, who pays merchants and other payees as they redeem the electronic value for hard currency. *Id.* In the Bank Secondary-Pre-Acquisition System, a depository institution purchases electronic value from a third party and then exchanges it for funds with its customers. *Id.*

[121] Federal Payments Made Through Financial Institutions by the Automated Clearing House Method, 50 Fed. Reg. 2405 (1987) (codified at 31 C.F.R. pt. 210). The term clearing house means "a payment mechanism through which participating institutions exchange funds electronically." *Id.* In the United States, the rule making body for commercial Automated Clearing House transactions is the National Automated Clearing House Association ("NACHA"). Federal Government Participation in the Automated Clearing House, 59 Fed. Reg. 50,112, 50,118 (1994) (to be codified at 31 C.F.R. pt. 210) (proposed Sept. 30, 1994).

[122] Electronic Fund Transfers, 61 Fed. Reg. 19,696 (1996) (to be codified at 12 C.F.R. pt. 205) (proposed May 2, 1996). On Thursday, May 2, 1996, the Federal Reserve Board published a proposed amendment to its Regulation E, which implements the Electronic Fund Transfer Act ("EFTA"). *Id.* The EFTA, codified at 15 U.S.C. § 1693 (1994), provides a basic framework sets forth the rights and responsibilities of parties participating in electronic fund transfer systems. *Id.* Through Regulation E, the Federal Reserve exercises its authority to enact regulations implementing the EFTA. *Id.* The EFTA and Regulation E apply to transactions involving ATM cards, POS (point of sale) terminals, automated clearinghouses, telephone bill-payment systems, and home banking programs. *Id.* They prescribe restrictions on unsolicited ATM card issuance, documentation and disclosure requirements, limitations on consumer liability for unauthorized transactions, procedures for error resolution, and certain rights related to preauthorized electronic fund transfers. *Id.* Although the amendment focuses primarily on applying Regulation E requirements to emerging banking technologies, the Board also spent considerable effort at outlining three specific electronic stored payment systems. *Id.* at 19,699-702. Coverage of SVCs under the EFTA and Regulation E depends on whether an SVC transaction involves an electronic transfer from the customer's account. *Id.* The Board defines an electronic fund transfer as "a transfer of funds initiated through electronic means . . . that results in a debit or credit to an

tem which the Federal Reserve Board[123] calls off-line[124] accountable, both the SVC chip and a central data facility record the available balance.[125] Parties do not contact the central database in order to consummate an electronic transaction, and transaction data is transmitted to the database only periodically.[126] In the off-line unaccountable stored value system, the transaction remains solely on the SVC chip.[127] After a merchant debits electronic value from an SVC, it remains on the merchant's database for a short time before transmission to the financial institution where the merchant can redeem the value for hard currency.[128] In on-line systems, a central data facility alone records the available balance and updates the record after each transaction.[129] Stored value cards operating on-line differ from traditional debit cards only in that the value associated with the card is limited to the amount that the cardholder has chosen to make available, and is only accessible through the card itself.[130]

account". *Id.* The Board defines account to mean "a demand deposit, savings, or other asset account - as described in the regulations of the Board - that is established primarily for personal, checking, and other deposit accounts [and] . . . accounts established by government agencies under electronic benefit transfer (EBT) programs . . . ." *Id.* at 19,698.

[123] *See* MACEY & MILLER, *supra* note 42, at 66 (stating that Federal Reserve Board, along with 12 Federal Reserve member banks, comprise Federal Reserve system which oversees bank holding companies and Federal Reserve member banks in United States).

[124] 61 Fed. Reg. at 19,698. The Federal Reserve Board defines off-line systems as operating,

> with transaction approval and data retention occurring only at the merchant level [where t]he balance of available funds may be stored only on the card itself as transactions occur, and transactions neither require nor receive authorization from a central database.

Id.

[125] *Id.* at 19,699 (noting that bank could serve as locus of central data facility).

[126] *See id.* (concluding that, because this system parallels debit card transactions and necessarily involves bank account, it falls under scope of Regulation E). Finding, however, that an unrestricted application of Regulation E requirements to these systems could potentially inhibit their development, the Board concluded that only a limited application would suffice. *Id.* at 19,699-701.

[127] *Id.* at 19,699-701.

[128] *See id.* at 19,701 (concluding that, since these systems lack centrally-operated database, they do not function like accounts and should not fall under Regulation E).

[129] General Counsel's Opinion No. 8, *supra* note 40, at 40,490.

[130] *See id.* at 19,699-702 (concluding that these systems fall under Regulation E requirements since they meet definition of consumer asset account). The Board also determined that compliance with Regulation E with only a few exceptions should not pose too great a burden on these systems since they already operate on-line. *Id. See also* Lorenz, *supra* note 120, at 1180 (stating that "[t]he crucial difference between on-line

b. Digital Coins

A digital coin is a unit of value identified by an encrypted serial number[131] and stored on a computer's hard drive[132] or a stored value card.[133] After a consumer transmits the coin to a merchant, the merchant redeems it for hard currency from the issuer.[134] The issuer can verify the coin's validity by checking its serial number.[135]

The Basle Committee[136] identifies two models of electronic coin payment systems.[137] In Basle's single-issuer model,[138] an issuer creates and distributes electronic coins to participating institutions, usually banks.[139] The participating institutions then issue the electronic coins to their customers by loading them onto SVCs or computer hard drives.[140] As the customers redeem

and off-line systems is that copying a card in an on-line system yields only an additional access device to a single store of funds, while in an off-line system, additional funds are created fraudulently by duplication.").

[131] *See* Froomkin, *supra* note 29, at 458 (describing role of encrypted serial number as preventive measure against forgery).

[132] *See* Smith & Wilson, *supra* note 50, at 1107 (noting that electronic coins are generally downloaded to software for use as payment in Internet transactions).

[133] Froomkin, *supra* note 29, at 466-67.

[134] *See id.* at 462 (discussing on-line and off-line clearing).

[135] *See id.* at 457 (noting structure of digital coin as serial number issued by bank and encrypted with bank's cryptographic key).

[136] Basle Core Principles for Effective Banking Supervision, *supra* note 2, at n.1. The Basle Committee is,

> [a] Committee of banking supervisory authorities which was established by the central-bank Governors of the Group of Ten countries in 1975. It consists of senior representatives of bank supervisory authorities and central banks from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, Netherlands, Sweden, Switzerland, United Kingdom, and the United States. It usually meets at the Bank for International Settlements in Basle, where its permanent Secretariat is located.

Id.

[137] Basle Report on Payment and Settlement Systems, *supra* note 2, at 34-37. Each model incorporates three general levels. *Id.* at 34. In the clearing and settlement domain, financial institutions, clearing houses and the central bank settle electronic transfers. *Id.* Electronic value is issued and acquired by consumers in the issuing/acquiring/operating domain. *Id.* The actual transactions between users take place in the retail domain. *Id.*

[138] *Id.* at 35.

[139] *See* Wilson, *supra* note 2, at 702 (noting that, in United States, federal banking regulators have indicated that issuers of electronic value do not fall under definition of banks, and thus are exempt from federal banking regulations, giving rise to question whether and by what agency non-bank entities providing bank-like services should be regulated).

[140] Basle Report on Payment and Settlement Systems, *supra* note 2, at 35; *see, e.g.*,

the coins for goods and services, merchants deposit them with their banks, other participating institutions.[141] These banks, in turn, claim the monetary value from the issuer, or system operator.[142] Consumers in this model can also transfer electronic coins between themselves using electronic wallets.[143]

The role of the system operator differs in the multiple-issuer model.[144] In this system, a number of different issuers distribute electronic coins to consumers.[145] Merchants who accepted the coins as payment deposit them with other issuers, who then contact the system operator.[146] The system operator consolidates the claims and transmits relevant information to the issuers.[147]

In addition to their different treatment of underlying funds, electronic coin payment systems operate either on-line[148] or off-line.[149] In order to conduct a transaction in an on-line system,

LYNCH & LUNDQUIST, *supra* note 3, at 26 (describing operation of CyberCash). A consumer using CyberCash must deposit money into a bank account especially designated for use as payment for Internet purchases. *Id.* As the consumer spends CyberCash funds online, CyberCash debits corresponding amounts of money from the designated account. *Id.*

[141] Basle Report on Payment and Settlement Systems, *supra* note 2, at 35.

[142] *Id. See* LYNCH & LUNDQUIST, *supra* note 3, at 111 (describing issuance of digital coin where consumer uses computer to generate random serial number and transmits it to bank which denotes value to serial number, debits appropriate sum from consumer's account, encrypts number and value with its cryptographic key, and transmits it back to consumer). After the consumer spends the digital coin, the merchant that accepted it as payment will transmit it back to the bank, which credits the merchant's account in the amount of the coin. *Id.* at 112.

[143] Basle Report on Payment and Settlement Systems, *supra* note 2, at 35.

[144] *Id.* at 36-37.

[145] *Id. See* LYNCH & LUNDQUIST, *supra* note 3, at 24 (stating that digital coin systems fall into either traveler's check model in which coins are generally accepted by merchants and cleared by issuer, and localized model, which operates similarly to store coupon that is accepted only at specific location determined by issuer).

[146] Basle Report on Payment and Settlement Systems, *supra* note 2, at 35.

[147] *Id. see* LYNCH & LUNDQUIST, *supra* note 3, at 29 (describing operation of DigiCash as typical multiple-issuer system, where any number of banks can issue DigiCash coins). Internet consumers wishing to use DigiCash coins can purchase them through a bank or an ATM machine. *Id.* DigiCash delivers the coins via e-mail in the form of encrypted sixty-four bit numbers, each corresponding to a specified amount of money. *Id.*

[148] *See* Stalder, *supra* note 104, at 8 (defining on-line as involving "a need to interact with a bank or another 'trusted third party' (via modem or network) to conduct a transaction.").

[149] *See id.* (defining off-line as "a transaction [that] can be conducted without having to involve the bank directly."); LYNCH & LUNDQUIST, *supra* note 3, at 109 (stating that ideal digital money system should include off-line clearing since it allows merchants to accept payment without depending on contact with central data facility).

parties must contact the issuer of the coin via modem or network.[150] The issuer then checks whether the proffered has not been spent more than once.[151] Because every on-line transaction involves this process, it generally offers more protection for the recipients and issuers of electronic coins from theft and fraud than off-line systems.[152] Transactions off-line generally do not involve contact with a bank or the issuer, and thus rely on other safeguards.[153] These may include securing the SVC from tampering or reverse engineering.[154] Cryptography constitutes the primary safeguard of digital cash used off-line.[155] Because off-line systems do not involve the additional step of contacting an issuer and performing a fraud check, they are generally much cheaper to implement than on-line systems.[156]

B. *Securing Electronic Money: Cryptography*

Cryptography existed centuries ago.[157] Julius Caesar, for example, used cryptography to send secret messages to his generals.[158] The system he used, now called the Caesar Cipher,[159] assigns a number to each letter in the alphabet, transcribes a message into corresponding numbers, and then adds the Cipher to each number in every word.[160] In the 1920s, encryption took

[150] Stalder, *supra* note 104, at 19-20.

[151] *See* Froomkin, *supra* note 29, at 463 (describing how on-line clearing prevents double spending by allowing banks to check coin proferred by payor against master list of spent coins).

[152] *See id.* at 462 (stating that "[p]reventing double-spending is relatively simple for an on-line clearing system; preventing [a criminal] from cheating a system that relies on off-line clearing is more difficult.").

[153] *See* Stalder, *supra* note 104, at 8 (noting that methods of safeguarding off-line digital money include hardware approach which involves using tamper-proof SVC chips and software approach which utilizes cryptography); Lorenz, *supra* note 120, at 1183 (citing Mondex as example of completely off-line digital payment system).

[154] Basle Report on Payment and Settlement Systems, *supra* note 2, at 14. Reverse engineering involves dissecting an SVC to determine how to construct a duplicate. *Id.*

[155] *See id.* at 14-17 and 57-64 (describing various benefits of using cryptography to safeguard digital money and electronic payment systems).

[156] Froomkin, *supra* note 29, at 463.

[157] Kerben, *supra* note 15, at 125.

[158] *Id.*

[159] *See* LYNCH & LUNDQUIST, *supra* note 3, at 250 (referring to Caesar Cipher system as substitution cipher).

[160] CRISIS REPORT, *supra* note 5, at 52; *see* LYNCH & LUNDQUIST, *supra* note , at 250 (describing ROT13 system that operates similarly by rotating each letter 13 places so that a is replaced by n, b by o, etc.).

place with the aid of machines which mechanically substituted a cipher for each letter in the message.[161] The most famous of these machines was the German enigma machine used by the Nazis to encrypt secret messages during World War II.[162] Cryptography did not rest on a firm mathematical foundation until 1949, when Claude Shannon developed the precursor of symmetric cryptography.[163] Today, cryptography exists in two primary forms, symmetric and asymmetric.[164] Whereas symmetric cryptography employs the same key to encrypt and decrypt a message, a message encrypted with an asymmetric key can only be decrypted with a distinct, private key.[165]

During the early development of cryptography, computing and communications were expensive and rare.[166] As information technology today develops on a global scale, the concomitant shared infrastructure and interdependence among computer-based systems create new risks.[167] For example, in 1994 an international group of criminals penetrated Citicorp's computerized electronic transfer system and moved approximately US$12 million[168] to other private accounts before being caught.[169] The robbery[170] starkly demonstrated the need for

[161] LYNCH & LUNDQUIST, *supra* note 3, at 253-54.

[162] *Id.*

[163] CRISIS REPORT, *supra* note 5, at 364.

[164] *See id.* at 375-76 (explaining encryption process in both symmetric and asymmetric systems); LYNCH & LUNDQUIST, *supra* note 3, at 72-86 (comparing security offered by symmetric and asymmetric cryptography and concluding that latter represents safer alternative).

[165] *See* LYNCH & LUNDQUIST, *supra* note 3, at 75 (stating that "[i]n contrast to [symmetric cryptography], the concept of [asymmetric cryptography] is based on the notion that cryptographic keys can come in pairs, and that one key cannot be derived from the other."); CRISIS REPORT, *supra* note 5, at 375 (stating that "[i]n symmetric cryptography, the encryption key is the same as the decryption key; thus, message privacy depends on the key being secret.").

[166] CRISIS REPORT, *supra* note 5, at 5.

[167] *Id.* at 22; *see id.* at 33 (noting that two former directors of DGSE, French intelligence service, stated that collecting economic information was top DGSE priority and that former DGSE Director Pierre Marion stated that he had initiated espionage program targeting U.S. businesses in order to keep French businesses internationally competitive).

[168] *See id.* (noting that electronic transfer systems allow thieves to transfer far greater amounts of money than could be physically taken away during stick up robbery).

[169] William Carley & Timothy O'Brien, *Cyber Caper: How Citicorp System Was Raided and Funds Moved Around World*, WALL ST. J., Sept. 12, 1995 at A1.

[170] *See* CRISIS REPORT, *supra* note 5, at n.21 (noting that World Wide Web offers ideal environment for stealing data through Trojan Horse ("TH") programs that are

data protection[171] in electronic commerce.[172] By ensuring confidentiality, authenticity, and integrity of devices, cryptography serves as the primary safeguard of electronic money and all software-based systems.[173] Because cryptography can emasculate

passed into workstation, obtain information, and periodically transmit it to TH originator).

[171] Council Directive No. 95/46, O.J. L 281/31 (1995) [hereinafter Data Protection Directive]. Protection of personal data has recently been an important topic of debate in the international community. In its Directive of October 24, 1995, the European Parliament and Council set forth guidelines ensuring that processing of personal data is accurate, up-to-date, relevant, and not excessive. *Id.* National laws under the Data Protection Directive must also permit individuals to erase or block the processing of incomplete or inaccurate data. *Id.* art. 12, O.J. L 281/31 at 42 (1995). In addition, each member state must establish an independent public authority to supervise the protection of personal data. *Id.* art. 28, O.J. L 281/31 at 47 (1995). Most importantly, the Data Protection Directive prohibits data transfers to countries found to offer inadequate data protection. *Id.* art. 25, O.J. L 281/31 at 45. Article 25 states:

> 1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer must take place only if . . . the third country in question ensures an adequate level of protection,
>
> . . .
>
> 4. Where the Commission finds . . . that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

Id. See Fred H. Cate, *Symposium: Data Protection Law and the European Union's Directive: The Challenge for the United States: The EU Data Protection Directive, Information Privacy, and the Public Interest,* 80 IOWA L. REV. 431, 437 (1995) (stating that Data Protection Directive presents significant challenge to United States, which does not have equivalent data protection infrastructure). Britain was the first to act under Article 25 by prohibiting the sale of a British mailing list to a United States direct mail organization. *Id.* at 438. Many believe, however, that the Data Protection Directive is simply another European attempt at threatening the U.S. dominance of the world information economy. *Id.* at 440.

[172] CRISIS REPORT, *supra* note 5, at 28-29. The CRISIS REPORT notes that U.S. firms increasingly operate in a global environment as tariffs among developed countries have been reduced by more than two thirds to around four percent and tarries among developing countries average 12.3% percent. *Id.* This expansion into the global marketplace has resulted in a greater dependence on the outside world. *Id.* More than a quarter of the U.S. GDP, for example, is now accounted for by trade in goods, services and returns on foreign investment. *Id.* In addition, this trend has resulted in the enormous recent growth of transnational corporations which operate across national borders. *Id.* There are around 300 such corporations based in the United States and almost 15,000 foreign affiliates. *Id.*

[173] Basle Report on Payment and Settlement Systems, *supra* note 2, at 1. Cryptography can help to

> [e]nsure the integrity of data (i.e., that data retrieved or received are identical to data originally stored or sent), to authenticate specific parties (i.e., that the purported sender or author of a message is indeed its real sender or author),

law enforcement efforts to police suspect electronic transmissions, commentators have proposed creating key escrow[174] authorities to maintain copies of cryptographic keys that can be subpoenaed during investigations.[175]

1. Symmetric Cryptography

Cryptography begins with a written message composed, for example, by Party A to be sent to Party B.[176] All letters in the message can be replaced by numbers.[177] Party A uses an encryption algorithm, a series of mathematical steps,[178] to scramble the written message according to the numeric representation of letters in the message.[179] The algorithm can be simple addition where A adds one to each number representing a letter in the message.[180] Thus A becomes B, B becomes C, . . . Y becomes Z, Z becomes space, space becomes comma, comma becomes period, and so on.[181] When B receives the message, B will need to know the decryption algorithm, subtraction in this case, and the corresponding key, which here is one.[182] The decryption algorithm

> to facilitate nonrepudiation, and to preserve the confidentiality of information that may have come improperly into the possession of unauthorized parties.

CRISIS REPORT, *supra* note 5, at 365; *see* LYNCH & LUNDQUIST, *supra* note 3, at 70-72 (describing role of cryptography in digital payment systems).

[174] *See* CRISIS REPORT, *supra* note 5, at 81 (explaining escrow agents as parties that hold copies of cryptographic keys for needs of government and corporate users).

[175] *See id.* at 170 (stating that taking no action to establish key escrow could negate government's authority to wiretap and collect intelligence for national security and foreign policy reasons).

[176] *See id.* at 374 (setting forth components of encryption process).

[177] *Id.*

[178] *See* LYNCH & LUNDQUIST, *supra* note 3, at 275 (defining algorithm as "set of steps for carrying out a calculation, a procedure or process usually carried out on a computer.").

[179] CRISIS REPORT, *supra* note 5, at 374.

[180] *Id.*

[181] *Id.* *See* LYNCH & LUNDQUIST, *supra* note 3, at 251-53 (discussing various ciphers.

[182] CRISIS REPORT, *supra* note 5, at 374; Steven Levy, *Wisecrackers*, WIRED, Mar. 1996, at 128. The key generation method may reveal valuable hints for guessing the actual key, and thus should be kept secret. *Id.* In late 1995, for example, David Wagner and Ian Goldberg, two graduate students at Berkely, cracked encryption used by Netscape by analyzing its random key-generator. *Id.* Because computers are engineered to work in precisely the same manner each time they execute a program, random key generators begin with a seed, a random number which ensures a lack of predictability. *Id.* Methods of choosing the seed include using the position of the mouse or any statistical data. *Id.* As Wagner and Goldberg found, Netscape chose its seeds by using the time of day and two fifteen bit Process Ids. *Id.* By choosing a specific time and then

and key will enable B to return the message to its original form by subtracting one from the numbers in the message and then translating the numbers back into letters, revealing the plaintext message written by A.[183] This simple encryption method is commonly called symmetric, secret key, or private key cryptography.[184] An example of a symmetric algorithm is the Data Encryption Standard ("DES") adopted by the United States Federal Government in 1977.[185] This standard uses fifty-six bit keys.[186] Parties using symmetric encryption must face two inherent security weaknesses.[187] First, both sender and recipient must trust each other not to reveal the key to third parties.[188] Second, because the key must somehow be transmitted from sender to recipient, it is vulnerable to interception by a third party.[189]

2. Asymmetric Cryptography

Weaknesses of symmetric cryptography are eliminated in asymmetric systems, also known as public key cryptography.[190]

guessing fifteen bit number combinations, they were able to find a Netscape key within one weekend. *Id.*

[183] CRISIS REPORT, *supra* note 5, at 374.

[184] *Id.* at 375; INFORMATION SECURITY COMMITTEE, ELECTRONIC COMMERCE AND INFORMATION TECHNOLOGY DIVISION, SECTION OF SCIENCE AND TECHNOLOGY, AMERICAN BAR ASSOCIATION, DIGITAL SIGNATURE GUIDELINES 8 (1996) [hereinafter A.B.A. DIGITAL SIGNATURE GUIDELINES]; Thomas W. Cashel, *Symposium: Financial Services: Security, Privacy, and Encryption,* 3 B.U. J. SCI. & TECH. L. 4 (1997); Basle Report on Payment and Settlement Systems, *supra* note 2, at 58.

[185] *See* Federal Information Processing Standard 46, Data Encryption Standard, 48 Fed. Reg. 41,062 (1983) (stating that Secretary of Commerce is authorized to establish uniform Federal automatic data processing standards under provisions of 40 U.S.C. § 759(f), and Executive Order 11717, 38 Fed. Reg. 12315). *Id.* The Data Encryption Standard was developed by IBM and issued by the National Bureau of Standards as the Federal Information Processing Standard ("FIPS") on January 15, 1977. *Id.*; *see also* CRISIS REPORT, *supra* note 5, at 417-18 (discussing development of Data Encryption Standard). In its Recommendation 4.1, the National Research Council stated that "[p]roducts providing confidentiality at a level that meets most general commercial requirements should be easily exportable. Today, products with encryption capabilities that incorporate the 56-bit DES algorithm provide this level of confidentiality and should be easily exportable." CRISIS REPORT, *supra* note 5, at 312.

[186] CRISIS REPORT, *supra* note 5, at table C1.

[187] *See* Charles R. Merrill, *A Cryptography Primer* (visited Aug. 1, 1997) <http://cla.org/RuhBook/chp2.htm> (also on file with the *Fordham International Law Journal*) (comparing mechanics of symmetric and asymmetric cryptography).

[188] *Id.*

[189] *Id.*

[190] A.B.A. DIGITAL SIGNATURE GUIDELINES, *supra* note 184, at 8; Cashel, *supra* note 184, ¶ 48; Basle Report on Payment and Settlement Systems, *supra* note 2, at 58.

Asymmetric cryptography is based on one-way functions.[191] For example, it is easy to multiply two prime numbers, but exceedingly difficult to compute the inverse function, which amounts to finding the product's factors.[192] In asymmetric systems, the two primes represent the private key known only to the sender, and the product of the two primes represents the public key, which can be freely distributed.[193] A message encrypted with the public key can only be decrypted with the private key, and vice-versa.[194] Because asymmetric encryption generally involves more complicated functions than symmetric systems, it requires more processing time and computer hardware.[195] The resulting higher cost has inhibited acceptance of asymmetric cryptography by SVC manufacturers.[196] An example of the asymmetric system is RSA,[197] developed by Ron Divest, Adi Shamir, and Leonard Adelman in 1977.[198] The RSA technology[199] is patented[200] and distributed by RSA Data Security Corporation.[201] There are currently more than eighty million copies of RSA programs installed worldwide.[202]

3. Digital Signatures

In addition to encoding messages, cryptography also plays an integral role in the mechanics of digital signatures.[203] Digital

[191] *See* CRISIS REPORT, *supra* note 5, at 376 (noting that one way functions are easy to compute but difficult to undo).

[192] *Id.*

[193] *Id.*

[194] Kerben, *supra* note 15, at 129; Basle Report on Payment and Settlement Systems, *supra* note 2, at 58; A.B.A. DIGITAL SIGNATURE GUIDELINES, *supra* note 184, at 8.

[195] *See* Basle Report on Payment and Settlement Systems, *supra* note 2, at 58 (comparing operation of DES and RSA systems).

[196] *Id.*

[197] *See* LYNCH & LUNDQUIST, *supra* note 3, at 277 (stating that RSA is an acronym for its creators, Rivest, Shamir and Adelman and generally refers to asymmetric cryptography).

[198] *See* Kerben, *supra* note 15, at 129-30 (describing development and mechanics of RSA).

[199] *See id.* (explaining mathematical process of calculating RSA keys).

[200] *See* CRISIS REPORT, *supra* note 5, at 228-30 (listing patent issues related to cryptography).

[201] *See* PR NEWSWIRE, *RSA Data Security to Provide Software to Secure Internet; DN-Ssafe(TM) Software Prevents Address Spoofing, Supports IETF's DNSSEC Standard*, Oct. 6, 1997 (stating that RSA Data Security Inc. is wholly owned subsidiary of Security Dynamics Technologies Inc., which sells wide range of software utilizing RSA algorithm).

[202] *Id.*

[203] *See* A. Michael Froomkin, *Symposium: Innovation and the Information Environ-*

signatures enable virtually foolproof authentication by encrypting a message digest created by a hash function with one's private key.[204] The hash function algorithm[205] translates an entire

ment: The Essential Role of Trusted Third Parties in Electronic Commerce, 75 OR. L. REV. 49 (1996) at 54-55 (discussing role of digital signature as authentication tool); Field, *supra* note 55, at 981-91 (discussing acceptance of digital signatures to authenticate electronic transmissions); A.B.A. DIGITAL SIGNATURE GUIDELINES, *supra* note 184, at 8-17 (describing operation of digital signatures); *Note by Secretariat: Planning of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Issues*, U.N. Commission on International Trade Law, 31st Sess., at ¶ 27, U.N. Doc. A/CN.9/WG.IV (1997) [hereinafter UN Secretariat Note on Digital Signatures] (explaining that individual signs electronic message by encrypting it with his or her private key). The recipient of a digitally-signed message will decrypt it with the sender's unique public key, thus verifying the sender's identity. *Id.* The United States federal government adopted a digital signature algorithm for use by all federal departments and agencies on May 19, 1994:

> [The Federal Digital Signature Standard] specifies a Digital Signature Algorithm (DSA) appropriate for applications requiring a digital rather than written signature. The DSA digital signature is a pair of large numbers represented in a computer as strings of binary digits. The digital signature is computed using a set of rules (i.e., the DSA) and a set of parameters such that the identity of the signatory and integrity of the data can be verified. The DSA provides the capability to generate and verify signatures. Signature verification makes use of a public key which corresponds to, but is not the same as, the private key. Each user possesses a private and public key pair. Public keys are assumed to be known to the public in general. Private keys are never shared. Anyone can verify the signature of a user by employing that user's public key. Signature generation can be performed only by the possessor of the user's private key.

Approval of Federal Information Processing Standards Publication 186, Digital Signature Standard (DES), 59 Fed. Reg. 26,208 (1994).

[204] *See* A.B.A. DIGITAL SIGNATURE GUIDELINES, *supra* note 184, at 8 (noting that digital signatures use asymmetric rather than symmetric cryptography).

[205] Approval of Federal Information Processing Standards Publication 180-1, Secure Hash Standard (SHS), 60 Fed. Reg. 19,211 (1995). Shortly after approving the DES, the federal government published the corresponding standard for a hash algorithm:

> This Standard specifies a secure hash algorithm, SHA-1, for computing a condensed representation of a message or a data file. When a message of any length < 2^{64} bits is input, the SHA-1 produces a 160-bit output called a message digest. The message digest can then be input to the Digital Signature Algorithm (DSA) which generates or verifies the signature for the message . . . . Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature.
>
> The SHA-1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest and the signature will fail to verify.

Id.

message into a single value called a hash result or checksum, which is normally much shorter than the message itself.[206] Because the hash function calculates the checksum of a particular message, the checksum result will uniquely reflect that message.[207] An individual signs the message by encoding the checksum with his or her private key and attaching the result to the message.[208] The verification of the digital signature involves decrypting the checksum with the sender's public key.[209] By using the hash function to compute the hash value anew and then comparing it with the hash value computed by the original sender, the receiver verifies that the message was unaltered in transit.[210]

Unlike written signatures, unique to the signer and normally difficult to forge, a public key by itself indicates no particular individual.[211] The receiver of a signed message, therefore, needs some other verification of the signer's identity besides tender of a public key.[212] A widely accepted means of resolving

[206] *See* A.B.A. DIGITAL SIGNATURE GUIDELINES, *supra* note 184, at 9 (defining hash function as algorithm that computes number based on particular message); CRISIS REPORT, *supra* note 5, at 367 (noting that checksums were originally used to detect errors in electronic transmissions).

[207] *See* A.B.A. DIGITAL SIGNATURE GUIDELINES, *supra* note 184, at 9 (noting that it is computationally infeasible to attempt to derive original message from hash value due to cost and time required).

[208] *See* CRISIS REPORT, *supra* note 5, at 367-68 (stating that private and public keys are mathematically related, so that checksum encrypted with private key can only be decrypted with public key). The recipient of a signed message will, for example, see the following:

> I, Mary Smith, promise to pay to the order of First Western Bank five thousand dollars and no cents ($5,000) on or before June 10, 1998, with interest at the rate of fifteen per cent (15%) per annum.
>
> Mary Smith, Maker
> </Signed>
> <Signature SigID=1 PsnID=smith082>
> 2AB3764578CC18946A29870F40198B240CD23
> 02B2349802DE002342B212990BA5330249C1D
> 20774C1622D39</Signature>

A.B.A. DIGITAL SIGNATURE GUIDELINES, *supra* note 184, at 12.

[209] A Michael Froomkin, *It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow,"* 1996 U. CHI. LEGAL F. 15, 29 n.64 (1996) (discussing digital signature process and noting that anyone who has sender's public key can verify integrity of signature).

[210] UN Secretariat Note on Digital Signatures, *supra* note 203, ¶ 26.

[211] *See* ABA DIGITAL SIGNATURE GUIDELINES, *supra* note 184, at 13 (stating that "a public and private key pair has no intrinsic association with any person.").

[212] *Id.*

this difficulty lies in the creation of trusted third parties, or certification authorities, to issue certificates authorizing the holder to use a specific key pair.[213] A party can check the authenticity of a certificate by verifying the certification authority's electronic signature using a public key verified by yet another certification authority.[214]

4. Cryptography and Digital Cash

Because each electronic coin contains a unique serial number authenticated by the issuer's electronic signature,[215] the coin's redemption links its original holder to the transaction if

[213] *See* UN Secretariat Note on Digital Signatures, *supra* note 203, ¶ 68(a)(1) (stating that "[a]n authorized certification authority shall keep a publicly accessible electronic register of certificates issued, indicating when the individual certificate was issued, when it expires or when it was suspended or revoked."); The A.B.A. Digital Signature Guidelines note that:

> A person seeking to verify a digital signature needs, at minimum, (1) the public key corresponding to the private key used to create the digital signature, and (2) reliable evidence that the public key (and thus the corresponding private key of the key pair) is identified with the signer. The basic purpose of the certificate is to serve both these needs in a reliable manner.

A.B.A. Digital Signature Guidelines, *supra* note 184, at comment 29; The Utah Digital Signature Act provides that:

> (1) A[n electronic] message is as valid, enforceable, and effective as if it had been written on paper, if it:
> (a) bears in its entirety a digital signature; and
> (b) that digital signature is verified by the public key listed in a certificate which:
> (I) was issued by a licensed certification authority; and
> (ii) was valid at the time the digital signature was created.
> (2) Nothing in this chapter precludes any message, document or record from being considered written or in writing under other applicable state law.

Utah Digital Signature Act, Utah Code Ann. § 46-3-403 (1997).

[214] A.B.A. Digital Signature Guidelines, *suprà* note 184, at 15; The UN Secretariat Note on Digital Signatures states that:

> [t]o assure the authenticity of the certificate with respect to both its contents and its source, the certification authority digitally signs it. The issuing certification authority's signature on the certificate can be verified by using the public key of the authorization authority listed in another certificate by another certification authority . . . , and that other certificate can in turn be authenticated by the public key listed in yet another certificate, and so on, until the person relying on the digital signature is adequately assured of its genuineness.

UN Secretariat Note on Digital Signature Guidelines, *supra* note 203, ¶ 37(a).

[215] *See* Law, *supra* note 2, at 1139 (stating that, in context of electronic coins, term bank can also refer to financial institution that issues and clears coins).

only the issuer keeps sufficient records.[216] Consumers can avoid this by using blinded coins.[217] The consumer creates a blinded coin by creating a serial number and then obscuring it with a random quantity called the blinding factor.[218] The bank signs the blinded coin with its private key in exchange for payment corresponding to the coin's value, not knowing either the identity of the consumer or the serial number of the coin.[219] The consumer then removes the blinding factor, revealing the coin's signed serial number, and forwards the coin to a merchant.[220] Unlike in the on-line system, where the merchant will not give up merchandise before ensuring the coin's validity, a blinded coin in the off-line system presents unique security concerns because neither the bank nor the merchant know the identity of the consumer.[221] The challenge-response protocol prevents the fraudulent use of blinded coins by requiring the consumer to forward a single piece of identifying information during each transaction.[222] The information remains encrypted during the first use.[223] If the consumer attempts to spend a previously-redeemed coin, it will reveal the personal information linking the criminal to the fraud.[224]

In addition to ensuring the anonymity of electronic coins, cryptography plays a central role in the administration of digital payment systems.[225] Called the cornerstone of digital money,

[216] *See* Froomkin, *supra* note 29, at 458 (discussing drawbacks of basic coin model).

[217] *See* id. at 460 (stating that "[u]sing 'blinded coins', [a consumer] can acquire digital cash with a unique serial number from a bank without allowing the bank to create a record of the coin's serial number").

[218] *See* Law, *supra* note 2, at 1139 (describing blinding process); Froomkin, *supra* note 29, at 460 (discussing the blinding factor); *See* DigiCash, *Numbers that are Money*, (1994) at 1 (visited Sept. 1, 1997) <http://www.eff.org/pub /. . .money/digicash.brochure> (also on file with the *Fordham International Law Journal*) [hereinafter DigiCash Brochure] (discussing how the user's equipment creates a blinded coin).

[219] DigiCash Brochure, *supra* note 218, at 2; Law, *supra* note 2, at 1141; Froomkin, *supra* note 29, at 460.

[220] DigiCash Brochure, *supra* note 218, at 2; Law, *supra* note 2, at 1141; Froomkin, *supra* note 29, at 460.

[221] Froomkin, *supra* note 29, at 463; Law, *supra* note 2 at 1141.

[222] *See* Froomkin, *supra* note 29, at 463 n.256 (discussing challenge-response protocol and developer, David Chaum).

[223] *See* Law, *supra* note 2, at 1142 (describing electronic cash payment system using challenge-response).

[224] *Id.*

[225] *See* Basle Report on Payment and Settlement Systems, *supra* note 2, at 14 (stating that "[c]ryptography is one of the most important components of fraud prevention

cryptography ensures the confidentiality of electronic payment messages.[226] Furthermore, cryptography prevents forgery of digital money by allowing issuers to certify its authenticity using digital signatures.[227] Digital signatures also allow the verification of the signatory's identity and the integrity of the transmission.[228] Finally, cryptographic authentication techniques can serve as access controls to various online systems.[229]

5. Security of the Cryptographic Code

The difficulty in breaking cryptography lies not in the complexity of the process, but rather in the magnitude of the task itself.[230] An intruder wishing to decrypt a message encrypted with a DES[231] key, for example, would have attempt 2^{56} different combinations to find the correct fifty-six bit key.[232] In 1977, Whitfield Diffie and Martin Hellman estimated that the exhaustive brute force[233] attack on DES would cost[234] approximately

in all electronic money systems"); *see also* LYNCH & LUNDQUIST, *supra* note 3, at 67 (stating that "[e]ncryption is essential to creating a secure environment for digital money; it is essential to creating digital money per se.").

[226] *See* LYNCH & LUNDQUIST, *supra* note 3, at 69 (noting that all Internet businesses rely on cryptography to ensure confidentiality of customer data); *see also* CRISIS REPORT, *supra* note 5, at 54 (asserting that confidentiality aspect of cryptography is solely responsible for controversy surrounding proposals to regulate it).

[227] *See* Basle Report on Payment and Settlement Systems, *supra* note 2, at 14 (discussing use of digital signatures in software-based electronic payment systems to prevent tampering with financial information such as available balance).

[228] *See* A.B.A. DIGITAL SIGNATURE GUIDELINES, *supra* note 184, at 10-11 (describing process of digital signature verification).

[229] *See* LYNCH & LUNDQUIST, *supra* note 3, at 70-71 (describing how encryption is used in operation of pin number to access one's bank account through ATM); *see also* CRISIS REPORT, *supra* note 5, at 56 (noting possible uses of cryptographic access controls such as dial-in ports and audit records).

[230] *See* CRISIS REPORT, *supra* note 5, at 378-83 (analyzing attacks on cryptographic systems).

[231] *See id.* at 227 (stating that U.S. government rejected RSA asymmetric technology as national digital signature standard in favor of DES, symmetric system which offered cost efficiency and royalty-free use). *See also id.* at 388 (describing DES as most widely studied cryptographic system).

[232] *Id.* at 388.

[233] *See* Froomkin, *supra* note 203, at 43 (stating that term brute force attack refers to method of finding cryptographic keys by using any combination of digits from range of possible keys until correct key is found).

[234] *See* CRISIS REPORT, *supra* note 5, at 385 (noting that, because microprocessor speed doubles on the average of once every 18 months and thus cost of computation decreases by factor of 10 every 5 to 7 years, computation which costs US$1 billion today may cost only US$10 in 50 years).

US$10,000 per key.[235] Only thirteen years later, M.J. Wiener estimated that a computer built with then-existing technology could produce a DES key in three and one half hours at a cost of around US$1 million per computer and US$80.00 per key.[236] Today, a standard US$10,000 machine could break a forty bit key in less than a second.[237] Commentators point out, however, that manufacturers of cryptographic technology will eventually eliminate all risk of code breaking by developing sufficiently long keys.[238] For example, a recent study found that, in order to decode a message encoded with a 1,024 bit key, one would need one hundred computers with eight megabytes of memory operating at one hundred MHz for 280,000 years.[239]

Because asymmetric cryptography uses the product of two prime numbers for encryption and the two original primes for decryption, cracking an asymmetric system involves factoring integers and finding discrete logarithms.[240] Unlike a brute force attack on DES, where attackers must try every possible combination of digits in a fifty-six bit number, the ease of factoring the public key to reveal the private key depends on the factoring method.[241] In 1995, for example a Bellcore team factored RSA-129, a 129 digit RSA key, in response to a 1977 challenge posted by Michael Gardner in his Scientific American mathematical games column.[242] Using a unique factoring method, Bellcore's Mas Par supercomputer, and the computers of 1600 volunteers recruited over the Internet, the Bellcore team factored RSA-129

[235] Whitfield Diffie & Martin Hellman, *Exhaustive Cryptanalysis of the NBS Data Encryption Standard,* COMPUTER, June 1977, at 74.

[236] CRISIS REPORT, *supra* note 5, at 388.

[237] Froomkin, *supra* note 203, at 43. *See* CRISIS REPORT, *supra* note 5, at 389 (suggesting that government oversight of large expenditures on computer technology could ensure that large corporations or criminal organizations do not attempt to gain access to encrypted information for illegal purposes).

[238] *See* CRISIS REPORT, *supra* note 5, at 380 n.17 (stressing that formulation of cryptographic key which would necessitate number of operations greater than practical limits of physics could ostensibly eliminate problem of advancement in computer technology); *id.* at 379-80 (stating that "[w]ith a sufficiently long key, even an eavesdropper with very extensive computer resources would have to take a very long time (longer than the age of the universe) to test all possible combinations").

[239] Kerben, *supra* note 15, at 129.

[240] *See id.* at 385 n.23 (explaining discrete logarithms).

[241] *Id.* at 386; *See* Levy, *supra* note 182 at 4 (discussing mathematical principles of encryption).

[242] *See* Taubes, *supra* note 15, at 776 (noting that asymmetric encryption was new concept when Gardner posted challenge).

in eight months.[243] Their 129 digit, 425 bit key cracked, RSA labs has noted that the current RSA tool kit allows development of 1,024 bit keys.[244] Discovery of new factoring algorithms and development of faster and more efficient computer technology will determine how long such keys will remain useful.[245]

6. Regulating Cryptography: Key Escrow

The conventional meaning of the word escrow implies the giving over of some thing of value for safekeeping along with precise instructions on how to do so.[246] In the context of cryptography, escrow represents the placement of a private cryptographic key with an agency or the government in order to ensure quick recovery when needed.[247] In addition to providing law enforcement with quick access to encrypted data, key escrow also serves as a means to retrieve lost or corrupted keys.[248] Furthermore, proponents of the widespread use of electronic signatures suggest that individuals' public keys, which allow identification of the signatory, should be issued and held in escrow by trusted third parties.[249] Having issued the signatory's key, a trusted third party, also called a certification authority,[250] can verify the signatory's true identity.[251]

Trusted third parties can also be useful in retrieving crypto-

[243] *See id.* (explaining operation of algorithm used to factor RSA-129). Measured in mips years, where one mips year represents a machine running for one year at one million instructions per second, the Bellcore RSA-129 experiment used about 5,000 mips years. Levy, *supra* note 182, at 5.

[244] Wirbel, *supra* note 15, at 1. Ronald Rivest of RSA labs claimed that a 400 digit number, which amounts to approximately 1320 bits, "may be 300 billion times more difficult" to crack than the 129 digit, 425 bit number. Taubes, *supra* note 15, at 776. *See* Kerben, *supra* note 15, at 129 (noting recent study finding that, in order to crack 1,024 bit key, one would need one hundred million computers with eight Megabytes of RAM operating at 100 MHz for 280,000 years).

[245] *See* Taubes, *supra* note 15, at 776 (stating that Bellcore team announced their intention to develop new factoring algorithms to factor larger numbers more efficiently at very press conference during which they presented solution to RSA-129).

[246] *See* CRISIS REPORT, *supra* note 5, at 167-69 (explaining escrowed encryption).

[247] *Id.* at 168.

[248] *Id.*

[249] *See* A.B.A. DIGITAL SIGNATURE GUIDELINES, *supra* note 184, at 14 (suggesting trusted third parties as solution to problems of falsification and repudiation of digital signatures).

[250] *See* CRISIS REPORT, *supra* note 5, at 355 (defining certification authority as "a specially established trusted organization that accepts the responsibilities of managing the certificate process by issuing, distributing, and verifying certificates.").

[251] A.B.A DIGITAL SIGNATURE GUIDELINES, *supra* note 184, at 14.

graphic keys through key management systems.[252] Key management differs from key escrow in that it does not require depositing cryptographic keys with a third party.[253] Rather, a key management recovery agent uses its own key to encrypt the private key that was used to encode a document.[254] The resulting encrypted private key, also known as the session key, is then attached to the transmission.[255] Law enforcement authorities seeking to decrypt this transmission need only require the key recovery agent to decrypt the session key.[256]

C. *Money Laundering*

In its 1996-1997, Report on Money Laundering Typologies,[257] the Financial Task Force on Money Laundering[258] ("FATF") noted the impossibility of gauging the true size of the money-laundering industry.[259] In 1988, estimates of the amount

[252] Jon William Toigo, *Key Recovery Spawns Debate; The Key Recovery Management Initiative May Hurt Encryption Sales Rather Than Help*, DATABASED WEB ADVISER, Aug. 1997, at 70.

[253] *Id.*

[254] *Id.*

[255] *Id. See* CRISIS REPORT, *supra* note 5, at 377 (discussing creation of key distribution center ("KDC") that holds copies of users' private keys that are used to encrypt session keys).

[256] *See* Toigo, *supra* note 252, at 70 (noting that although key management does not require users to hand over copies of cryptographic keys to government, end result is same and thus implicates same privacy issues).

[257] 1997 FATF Report, *supra* note 4.

[258] *See* Lisa A. Barbot, *Comments: Money Laundering: An International Challenge*, 3 TUL. J. INT'L & COMP. L. 161 (1995) (noting that Financial Action Task Force on Money Laundering ("FATF") was established at Paris G-7 Summit in 1989). The FATF functions to:

> . . . assess the results of cooperation already undertaken in order to prevent the utilization of the banking system and financial institutions for the purpose of money laundering, and to consider additional preventive efforts in this field, including the adoption of the legal and regulatory systems so as to enhance multilateral judicial assistance.

Paris Economic Summit: Economic Declaration July 16, 1989, *reprinted in* 28 I.L.M. 1293, 1299 (1989). Today, the twenty-six FATF member countries include Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, Turkey, United Kingdom, and United States. 1997 FATF Report, *supra* note 4, at 1. The European Commission and the Gulf Cooperation Council are also members. *Id.*

[259] *See* 1997 FATF Report, *supra* note 4, at 3 (stating that FATF Members estimated size of money laundering problem based on amount of money confiscated from money launderers and that such estimates do not necessarily reflect total amount of money laundered).

of money laundered in the United States alone were as high as US$170 billion annually.[260] Similar estimates in 1994 set the amount at around US$300 billion.[261] Traditional means of detecting and eliminating money laundering include imposing reporting requirements on financial institutions that provide money transfer services.[262] Because digital payment systems operate without such services, they permit money launderers to ply their trade with minimal risk of detection.[263]

1. The Money Laundering Process

Money laundering involves making funds obtained through criminal activity appear as legitimate earnings.[264] The entire

[260] Baldwin, *supra* note 78, at 415.

[261] Sultzer, *supra* note 16, at 143.

[262] *See generally id.* at 151-84 (discussing money laundering legislation in United States mandating financial institutions to maintain reports and records to facilitate investigations or legal proceedings); Barbot, *supra* note 258, at 170-81 (discussing anti-money laundering initiatives of United Nations, Financial Action Task Force, Basle Committee and European Community which rely on shared access to data maintained by financial institutions).

[263] *See, e.g.*, *Electronic Currency: Consumer Convenience, or Money Laundering Incentive?*, NATIONAL ASSOCIATION OF ATTORNEYS GENERAL FINANCIAL CRIMES REPORT, Oct. 1997, at 11 (stating that "[e]lectronic transfers become the preferred money laundering technique because once currency enters the electronic system, it can be transferred to dozens of banks in as little as 24 hours, making it very difficult to create a paper trail."); *Security: Money Laundering and the Net*, THE AMERICAN BANKER, May 12, 1997, at 18 (noting experts' concern that "[i]f not today, as electronic cash systems are popularized, criminals could be lured easily by the instantaneous and potentially anonymous means by which illicit funds could be moved, domestically or electronically.").

[264] *See id.* at 143 (stating that "money laundering sustains every criminal activity engaged in for profit, which is to say all crime but crimes of passion or vengeance."); Baldwin, *supra* note 78, at 413 (noting that some nations cater to criminals' money laundering needs to gain direct economic benefit). The European Council has defined international money-laundering to mean:

> -the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action,
>
> -the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity of from an act of participation in such activity,
>
> -the acquisition, possession or use of property, knowing, at the same time of receipt, that such property was derived from criminal activity or from an act of participation in such activity,
>
> . . . .

Council Directive 91/308, *supra* note 11, art. 1, O.J. L 166/77, at 79 (1991).

process takes place in three steps often termed placement, layering, and integration.[265] Placement, the first step in the money laundering process, involves depositing the money at a legitimate business or financial institution.[266] Associating the money with a legitimate source facilitates obscuring its origin in the next stage, layering.[267] Layering involves transferring the money between a large number of financial institutions and shell[268] legal entities, making it difficult to trace to an illegitimate source.[269] In a recent case,[270] for example, drug money was picked up in various U.S. cities and deposited in different

[265] Sultzer, *supra* note 16, at 148; *See* Baldwin, *supra* note 78, at 418 (describing laundering process as including externalizing, agitation, and repatriation).

[266] Sultzer, *supra* note 16, at 149.

[267] *Id.*

[268] *See* Barbot, *supra* note 258, at 167 (stating that money launderers use shell or letter box corporations set up in jurisdictions offering significant financial privacy to serve as conduits for transferring ill-gotten funds to legitimate institutions).

[269] Sultzer, *supra* note 16, at 149.

[270] *See* Daniel M. Laifer, *Putting the Super Back in the Supervision of International Banking, Post-BCCI* 60 FORDHAM L. REV. 467, 484 (1992) (describing similar case where Bank of Credit and Commerce International ("BCCI") laundered more than thirty two million U.S. dollars in United States). The failure of the $20 billion BCCI on July 5, 1991 marked the largest bank failure in international history. Duncan E. Alford, *Basle Committee Minimum Standards: International Regulatory Response to the Failure of BCCI* 26 GEO. WASH. J. INT'L L. & ECON. 241 (1992). Although BCCI's holding company and one of its major banking subsidiaries were chartered in Luxembourg, neither actually conducted business in that country and thus, under the existing laws, banking regulators in Luxembourg were not required to police BCCI's global operations. Laifer, *supra*, at 481. Having "no clear home country supervision," BCCI escaped regulatory oversight altogether. Alford, *supra*, at 263. By making bad loans and engaging in a wide range of fraud and criminal activity, BCCI incurred liabilities amounting to US$10.641 billion. *Id.* at 264. In direct response to the gross lack of international supervision which lead to BCCI's failure, the Basle Committee issued its Minimum Standards for the Supervision of International Banking Groups and Their Cross-Border Establishments in July of 1992. *Id.* at 266. The minimum standards include:

1. All international banking groups and international banks should be supervised by a home country authority that capably performs consolidated supervision.
2. The creation of cross-border banking should receive the prior consent of both the host country supervisory authority and the bank's and, if different, banking group's home country supervisory authority.
3. Supervisory authorities should possess the right to gather information from the cross-border banking establishments of the banks or banking grouped for which they are the home country supervisor.
4. If a host country authority determines that any of the foregoing minimum standards is not met to satisfaction, that authority could impose restrictive measures necessary to satisfy its prudential concerns consistent with these minimum standards, including the prohibition of creation of banking establishments.

banks.[271] The funds were wire-transferred from those banks to a bank account in Florida and then wire-transferred via New York to Luxembourg and London where they were converted to certificates of deposit.[272] The certificates were used as collateral for a Nassau bank loan.[273] Sufficiently layered, the laundered money, now in the form of loan proceeds, could be reintegrated into the legitimate financial world.[274]

2. Traditional Money Laundering Control Measures

Ratified in Vienna in October of 1990, the U.N. Convention Against Illicit Traffic[275] ("U.N. Convention") represents one of the earliest international efforts to combat money laundering.[276] Under Article 3(1) of the U.N. Convention, countries must criminalize cross-border money laundering schemes[277] and en-

Basle Committee, Minimum Standards for the Supervision of International Banking Groups and Their Cross-Border Establishments (July 1992).

[271] Sultzer, *supra* note 16, at 151 n.31.

[272] *Id.*

[273] *Id.*

[274] *Id. See* Barbot, *supra* note 258, at 168 (stating that "once the money is clean, it is usually wired from the local international branch to a legitimate bank . . . [and then] back to the United States").

[275] UN Convention Against Illicit Traffic, *supra* note 11, 28 I.L.M. 493 (1989).

[276] Frank C. Razzano, *American Money Laundering Statutes: The Case for a Worldwide System of Baking Compliance Programs*, 3 D.C.L. J. INT'L L. & PRAC. 277, 303 (1994). At the December 20, 1988 signing ceremony, the following nations signed the UN Convention Against Illicit Traffic: Afghanistan, Algeria, Argentina, Bahamas, Bolivia, Brazil, Canada, Chile, China, Colombia, Cote d'Ivore, Cyprus, Denmark, Egypt, Ghana, Guatemala, Holy See, Honduras, Iran, Israel, Italy, Jordan, Malaysia, Mauritania, Mauritius, Nicaragua, Norway, Panama, Paraguay, Peru, Philippines, Senegal, Spain, Suriname, Sweden, Turkey, United Kingdom, United Republic of Tanzania, United States, Venezuela, Yemen, Yugoslavia, and Zaire. UN Convention Against Illicit Traffic, *supra* note 11, 28 I.L.M. at 493. Morocco signed on December 28, 1988. *Id.*

[277] UN Convention Against Illicit Traffic, *supra* note 11, 28 I.L.M. at 500. The pertinent part of Article 3 states:

> 1. Each Party shall adopt such measures as may be necessary to establish as criminal offences under its domestic law, when committed internationally:
>
> . . .
>
> (b) (I) The conversion or transfer of property, knowing that such property is derived from any offence [involving psychotropic substances as outlined in Art. 3(1)(a)] for the purpose of concealing or disguising the illicit origin of the property or of assigning any person who is involved in the commission of such an offence or offences to evade the legal consequences of his action;
>
> (ii) The concealment or disguise of the true nature source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from

act measures allowing law enforcement officers to confiscate drug money.[278] In addition, parties under the U.N. Convention must work together by maintaining communication and assisting in judicial proceedings and investigations.[279] The U.N. Convention also allows signatories to place the burden of proof regarding the origin of allegedly illicit property on the property owner,[280] and, most importantly, limits bank secrecy and confidentiality laws.[281]

Under the Council of Europe Convention held in Strasbourg in 1990,[282] signatory nations[283] rallied together to launch a united front against money laundering.[284] The Council of Eu-

> offences [involving psychotropic substances as outlined in Art. 3(1)(a)].

Id.

[278] *Id.* 28 I.L.M. at 504. Article 5, paragraph 1 of the Convention mandates that:

> Each party shall adopt measures as may be necessary to enable confiscation of:
> (a) Proceeds derived from offences [involving psychotropic substances as outlined in Art. 3(1)];
> . . .

Id.

[279] *Id.* 28 I.L.M. at 508. The Convention outlines the extent to which the signatory nations must cooperate in Article 7:

> 1. The parties shall afford one another, pursuant to this article, the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to criminal offences [involving psychotropic substances as outlined in art. 3 par. 1].
> 2. Mutual legal assistance to be afforded in accordance with this article may be requested for any of the following purposes:
> (a) Taking evidence or statements from persons;
> (b) Effecting service of judicial documents;
> (c) Executing searches and seizures;
> (d) Examining objects and sites;
> (e) Providing information and evidentiary items;
> (f) Providing originals or certified copies of relevant documents and records, including bank, financial, corporate or business records;
> (g) Identifying or tracing proceeds, property, instrumentalities or other things for evidentiary purposes.
> . . .

Id.

[280] *Id.* 28 I.L.M. at 506.

[281] *See id.* 28 I.L.M. at 509 (stating that "[a] party shall not decline to render mutual assistance under this article on the ground of bank secrecy.").

[282] Council of Europe Convention, *supra* note 11, 30 I.L.M 148 (1991).

[283] *Id.* Countries which signed the council of Europe Convention on November 8, 1990 included Belgium, Cyprus, Denmark, Federal Republic of Germany, Iceland, Italy, the Netherlands, Norway, Portugal, Spain, Sweden, and the United Kingdom. *Id.*

[284] EC Ministers to Adopt Formally Money Laundering Law, REUTER LIBR. REP., Jun. 7, 1991.

rope Convention echoes the U.N. Convention by requiring nations to cooperate with one another in detecting and confiscating illicit property[285] and prosecuting money launderers.[286] The Council of Europe Convention also mandates that nations actively monitor telecommunications and minimize the extent to which bank secrecy laws could hinder efforts to curb money laundering.[287]

The most recent multinational effort to prevent money laundering through financial networks is Council Directive 91/308.[288] Also like the U.N. Convention, Council Directive 91/308 notes that measures enacted to curb money laundering will work only if nations cooperate in a joint effort.[289] Deriving its definition of money laundering from the U.N. Convention,[290] Council

[285] Council of Europe Convention, *supra* note 11, 30 I.L.M. 148, 152 (1991). Laundering offenses which the Convention directs signatory nations to criminalize include:

> (a) the conversion or transfer of property, knowing that such property is [economic benefit derived from criminal activity], for the purpose of concealing or disguising the illicit origin of the property . . . .
> (b) the concealment or disguise of the true nature, source, disposition, movement, rights with respect to , or ownership of, property, knowing that such property is [economic benefit derived from criminal activity] . . .

Id.

[286] *See id.* 30 I.L.M. at 153 (stating that "[t]he parties shall co-operate with each other to the widest extent possible for the purposes of investigations and proceedings aiming at the confiscation of instrumentalities and [any economic advantage derived from criminal activity"). *See also id.* 30 I.L.M. at 152 (stating that "[e]ach party may adopt such measures as it considers necessary to establish also as offences under its domestic law all or some of [the laundering crimes outlined by the Convention]").

[287] *Id.* 30 I.L.M. at 151. Article 4 of the Council of Europe Convention states that:

> 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized in order to carry out [law enforcement].
> 2. Each Party shall consider adopting such legislative and other measures as may be necessary to enable it to use special investigative techniques facilitating the identification and tracing of proceeds and the gathering of evidence related thereto. Such techniques may include monitoring orders, observation, interception of telecommunications, access to computer systems and orders to produce specific documents.

Id.

[288] Council Directive 91/308, *supra* note 11, O.J. L 166/77 (1991).

[289] Barbot, *supra* note 258, at 179.

[290] *See* Council Directive 91/308, *supra* note 11, art. 1, O.J. L 166/77, at 79 (1991) (defining "money laundering"); UN Convention Against Illicit Traffic, *supra* note 11, art. 3 (setting forth criminal offenses, including money laundering, to be criminalized by signatory nations).

Directive 91/308 mandates that Member States require financial institutions[291] to obtain documents identifying customers involved in transactions of 15,000 ECU or more.[292] Council Directive 91/308 also imposes a duty on financial institutions to investigate any transactions which appear to involve illicit funds.[293] In addition, Member States must establish authorities responsible for combating money laundering and laws providing that financial institutions shall cooperate with the authorities by divulging pertinent information and refraining from carrying out questionable transactions.[294] Furthermore, Member States must ensure that financial institutions develop proper internal safeguards to detect and report instances of apparent money laun-

[291] Council Directive 91/308, *supra* note 11, art. 1, O.J. L 166/77, at 79 (1991). The Directive defines financial institution to include:

> . . . an undertaking other than a credit institution whose principal activity is to carry out one or more of the operations included in numbers 2 to 12 and number 14 of the list annexed to Directive 89/646/EEC, or an insurance company duly authorized in accordance with Directive 79/267/EEC, as last amended by Directive 90/619/EEC, in so far as it carries out activities covered by that Directive; this definition includes branches located in the Community of financial institutions whose head offices are outside the Community.

Id. The operations in the annex to Directive 89/646/EEC include those institutions which (1) engage in safe custody services, (2) lending (including consumer credit, mortgage credit, and the financing of commercial transactions), (3) financial leasing, (4) money transmission services, (5) issuing and administering means of payment (credit cards, travelers' checks, and banker's drafts), (6) guarantees and commitments, (7) trading for own account or for that of their customers in money market instruments, foreign exchange, financial futures and options, exchange and interest rate instruments, and transferable securities, (8) participating in share issues, (9) advice to undertakings on capital structure, industrial strategy and related issues such as mergers and the purchase of undertakings, (10) money broking, (11) portfolio management and advice, and (12) safekeeping and administration of securities. Second Banking Directive No. 89/646, art. 18, O.J. L 386/9 at 13 (1989).

[292] Council Directive 91/308, *supra* note 11, art. 3, O.J. L 166/77, at 79-80 (1991).

[293] *See id.* art. 5, O.J. L 166/77, at 80 (1991) (stating that "[m]ember States shall ensure that credit and financial institutions examine with special attention any transaction which they regard as particularly likely, by its nature to be related to money laundering").

[294] *See id.* art. 3, O.J. L 166/77, at 79-80 (1991) (stating that "[m]ember States shall ensure that money laundering . . . is prohibited"); *id.* art. 4, O.J. L 166/77, at 80 (1991) (stating that "[m]ember States shall ensure that credit and financial institutions and their directors and employees cooperate fully with the authorities responsible for combating money laundering . . . ."); *id.* art. 7, O.J. L 166/77, at 80 (1991) (stating that "[m]ember States shall ensure that credit and financial institutions refrain from carrying out transactions which they know or suspect to be related to money laundering . . . .").

dering.[295]

To facilitate international cooperation in combating money laundering, the United States and other nations have ratified Mutual Assistance Treaties ("MLATs").[296] MLATs expedite the process of uncovering and prosecuting international money laundering by, for example, creating binding obligations between nations to provide key evidence despite domestic privacy laws.[297] Generally, MLATs contain provisions enabling the requesting state to secure relevant documentation and immobilize assets obtained through alleged criminal activity.[298]

[295] *Id.* art. 11, O.J. L 166/77, at 81 (1991). Article 11 of Council Directive 91/308 states that:

> Member States shall ensure that credit and financial institutions:
>
> 1. Establish adequate procedures of internal control and communication in order to forestall and prevent operations related to money laundering,
> 2. Take appropriate measures so that their employees are aware of the provisions contained in this Directive. These measures shall include participation of their relevant employees in special training programmes to help them recognize operations which may be related to money laundering as well as to instruct them as to how to proceed in such cases.

Id.

[296] Razzano, *supra* note 276, at 301; Sultzer, *supra* note 16, at 209.

[297] *Id.* at 301.

[298] The Treaty Between the United States of America and the Italian Republic on Mutual Assistance in Criminal Matters, June 11, 1984, 24 I.L.M. 1509, 1536 [hereinafter Mutual Assistance Treaty Between the United States and Italy]. For example, article 18 of the Mutual Assistance Treaty between the United States and Italy provides that:

> 1. In emergency situations, the Requested State shall have authority to immobilize assets found in that State which are subject to forfeiture.
> 2. Following such judicial proceedings as would be required under the laws of the Requested State, that State shall have the authority to order the forfeiture to the Requesting State of assets immobilized pursuant to paragraph 1 of this Article.

Id. art. 18, 24 I.L.M. at 1541-42. Article 1 of assistance treaty between the United States and the Netherlands exemplifies the usual extent of assistance guaranteed by an MLAT:

> 1. The Contracting Parties undertake to afford each other, upon request and in accordance with the provisions of this Treaty, mutual assistance in criminal investigations and proceedings.
> 2. Assistance shall include, but not be limited to:
>   a. locating persons;
>   b. serving documents;
>   c. providing records;
>   d. taking the testimony or statements of persons;
>   e. producing documents;
>   f. executing requests for search and seizure; and
>   g. transferring persons in custody for testimonial purposes.

Netherlands-United States: Treaty on Mutual Legal Assistance, June 12, 1981, 21 I.L.M. 48, 50.

By enacting the Bank Secrecy Act of 1970[299] ("BSA"), the U.S. Government recognized the importance of maintaining a paper trail whereby law enforcement could trace large transactions by financial institutions.[300] Under the BSA, financial institutions conducting transactions on behalf of a single individual involving US$10,000 or more in the aggregate must file an Internal Revenue Service[301] ("IRS") Form 4789 Currency Transaction Report ("CTR").[302] In addition, the BSA requires that any person transporting monetary instruments worth more than US$10,000 across United States borders must so declare by filing a Currency and Monetary Instrument Report ("CMIR").[303] The BSA also requires financial institutions to generally report suspicious transactions.[304] No BSA provision, however, imposes record keeping or reporting requirements on wire transfers not involving the physical transfer of currency.[305]

[299] Pub. L. No, 91-598, 84 Stat. 1114-1124 (codified as amended at 31 U.S.C. §§ 5311-5344).

[300] *See* Baldwin, *supra* note 78, at 424 (discussing legislation passed to combat money laundering). Under the Bank Secrecy Act, financial institution means: (1) an insured bank, (2) a commercial bank or trust company, (3) a private banker, (4) an agency or branch of a foreign bank in the United States, (5) an insured institution, (6) a thrift institution, (7) a broker or dealer registered with the SEC, (8) a broker or dealer in securities or commodities, (9) an investment banker or investment company, (10) a currency exchange, (11) an issuer, redeemer, or cashier of traveler's checks, (12) an operator of a credit card system, (13) an insurance company, (14) a dealer in precious metals, stones, or jewels, (15) a pawnbroker, (16) a loan or finance company, (17) a travel agency, (18) a licensed sender of money, (19) a telegraph company, (20) a business engaged in car, airplane, or boat sales, (21) persons involved in real estate closings or settlements, (22) The U.S. Postal Service, (23) an agency of the U.S., state, or local government carrying out a duty or power of a business described in § 5312(a)(2), (24) any business that the Secretary of the Treasury determines is an activity under § 5312(a)(2), and (25) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters. The Bank Secrecy Act, 31 U.S.C. § 5312(a)(2) (1994).

[301] *See* John C. Chommie, The Internal Revenue Service 9 (1970) (stating that U.S. Congress established Office of Commissioner of Internal Revenue under Revenue Act of 1862 in order to implement new, broader tax system).

[302] 31 U.S.C. § 5313 (1994); 31 C.F.R. § §103.33-.34; *see* Sultzer, *supra* note 16, at 152 (discussing BSA Currency Transaction Report ("CTR") filing requirement); Barbot, *supra* note 258, at 188 (noting that financial institutions falling under BSA filed more than 30 million CTRs between 1970 and 1995).

[303] 31 U.S.C. § 5316(a)(1) (1994); *see* Sultzer, *supra* note 16, at 152 n.50 (discussing history of Currency and Monetary Instrument Report ("CMIR") requirement). The CMIR does not apply to cross-border wire transfers. *Id.* at 152.

[304] *See* Baldwin, *supra* note 78, at 425 (explaining BSA reporting requirements).

[305] *See* Fletcher N. Baldwin, Jr. & Robert J. Munro, *Money Laundering and the 1995 Wire Transfer Regulations: Are Regulations Alone Adequate to Take the Profit Out of Illicit Wire*

Soon after the enactment of the BSA, criminals quickly found ways to escape the reporting requirement by smurfing[306] or structuring[307] payments, which simply involved transferring an amount less than US$10,000 per transaction.[308] To remedy this apparent weakness, Congress amended[309] the BSA with the Money Laundering Control Act of 1986 ("MLCA").[310] The MLCA criminalized structuring payments and inhibiting a financial institution's efforts to satisfy the reporting requirements.[311]

Also around this time, law enforcement authorities began to note the internationalization of money laundering and the increasing difficulty and cost of following the paper trail of illegitimate money.[312] Criminals' use of wire transfer systems, unregulated until 1995, represented the main reason for this increased

Transfers?, *in* 1 MONEY LAUNDERING, ASSET FORFEITURE AND INTERNATIONAL FINANCIAL CRIMES 15 (1995) (discussing wire transfers before BSA reporting requirements).

[306] *See* Barbot, *supra* note 258, at 186 (defining smurfing as intentionally arranging transactions to circumvent reporting requirements).

[307] *See* Sultzer, *supra* note 16, at 158 (discussing drawbacks of BSA resulting from structuring).

[308] Barbot, *supra* note 258, at 186.

[309] *See* Baldwin, *supra* note 78, at 425 (discussing legislative history of BSA). The BSA was amended by the Comprehensive Crime Control Act of 1984, Pub. L. 98-473, Title II, Oct. 12, 1984, the Money Laundering Control Act of 1986, 18 U.S.C. 1956-1957, the Anti-Drug Abuse Act of 1988, Pub. L. 100-690, Nov. 18, 1988, and the Annunzio-Wylie Anti-Money Laundering Act of 1992, Pub. L. No. 102-550. *Id.*

[310] Pub. L. No. 99-570, 100 Stat. 3207-18 (codified as amended at 18 U.S.C. §§ 1956-1957, 31 U.S.C. §§ 5324-5326); *see also* Sultzer, *supra* note 16, at 158 (discussing congressional intent in passing the Money Laundering Control Act of 1986 ("MLCA")).

[311] 31 U.S.C. § 5324 (1994). This section provides that:

> (a) . . . No person shall for the purpose of evading the reporting requirements . . .
>
> (1) cause or attempt to cause a domestic financial institution to fail to file a report under section 5313(a) or 5325 or any regulation prescribed under any such section;
>
> (2) cause or attempt to cause a domestic financial institution to file a report . . . that contains a material omission or misstatement of fact; or
>
> (3) structure or assist in structuring, or attempt to structure or assist in structuring, any transaction with one or more domestic financial institutions.

Id. After the Supreme Court held in Ratzlaf v. United States, 114 S. Ct. 655 (1994), that convictions under this section required willful violation, Congress explicitly dispensed with the willfulness requirement by passing the Money Laundering Suppression Act of 1994, Pub. L. No. 103-325 § 411, 108 Stat. 2160, 2253 (1994). Sultzer, *supra* note 16, at 168.

[312] *See* Dilwyn Griffiths, *International Efforts to Combat Money Laundering: Developments and Prospects*, 19 COMMONWEALTH LAW BULLETIN 1824 (1993) (stating that money laundering problem has grown in size and complexity since 1989).

burden on law enforcement.[313] The instantaneous economy created by newly-emerging information and electronic finance technologies threatened to render the existing money laundering safeguards utterly useless.[314] In 1995, the Financial Crimes Enforcement Network[315] ("FinCen") and the Federal Reserve Board jointly enacted an amendment to the BSA regulations to facilitate tracing money laundering via wire transfer systems.[316] The new regulations require financial institutions[317] conducting wire transfers to maintain detailed records[318] concerning pay-

[313] *See* Barbot, *supra* note 258, at 193 (stating that wire transfers resulted in internationalization of money laundering).

[314] *See id.* at 196 (noting money laundering prevention difficulties caused by new technologies).

[315] *See* Sultzer, *supra* note 16, at 179 (describing FinCen). FinCen, an acronym for the Financial Crimes Enforcement Network, is one of six Treasury Department agencies active in the fight against money laundering. *Id.* Established in 1990, this 200-employee organization collects data and analyses issues related to financial crimes and money laundering. *Id.* at 180.

[316] *See* 58 Fed. Reg. 46,014-015 (1993) (stating purpose of new regulations as prevention of money laundering via wire transfers).

[317] Financial Record keeping and Reporting of Currency and Transactions, 31 C.F.R. § 103.11(n). The regulations define financial institution to mean:

> [e]ach agent, agency, branch, or office within the United States of any person doing business, whether or not on a regular basis or as an organized business concern, in one or more of the capacities listed below:
>
> (1) A bank (except bank credit card systems);
>
> (2) A broker or dealer in securities;
>
> (3) A currency dealer or exchanger, including a person engaged in the business of a check cashier;
>
> (4) An issuer, seller, or redeemer of traveler's checks or money orders except as a selling agent exclusively who does not sell more than $150,000 of such instruments within any given 30-day period;
>
> (5) A licensed transmitter of funds, or other person engaged in the business of transmitting funds;
>
> (6) A telegraph company;
>
> . . .

Id. The regulation defines funds transfer as "[t]he series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order . . . . ". *Id.* § 103.11(q). The definition excludes fund transfers governed by the Electronic Funds Transfer Act of 1978 and all money transfers made by means of an automated clearinghouse. *Id.*

[318] Amendment to the Bank Secrecy Act Regulations Relating to Record Keeping for Funds Transfers and Transmittals of Funds by Financial Institutions, 60 Fed. Reg. 220, 229-31 (1995). The regulations require banks and non-bank financial institutions transmitting US$3,000 or more to keep records relating to the payment order including:

> (A) The name and address of the originator;
>
> (B) The amount of the payment order;
>
> (C) The execution date of the payment order;

ment orders for a period of five years.[319] Previously unregulated payment order transactions including those conducted by FedWire, CHIPS, and SWIFT fall under the new regulations.[320]

3. The New Challenge for Law Enforcement: Laundering Digital Money

Commentators and legal authorities around the world look on with increasing anxiety as technological innovations drive the development of payment systems that threaten to emasculate current money laundering safeguards.[321] For example, the FATF has recommended that nations reevaluate their exiting money laundering controls to determine whether they provide

> (D) Any payment instructions received from the originator with the payment order;
>
> (E) The identity of the beneficiary's bank; and
>
> (F) [any other available information about the recipient of the funds]

Id. The regulations also require an institution acting as intermediary to keep a copy of the payment order. *Id.* at 229-30.

[319] *Id.* at 228. The regulations define payment order to mean:

> [a]n instruction of a sender to a receiving bank, transmitted orally, electronically, or in writing, to pay, or to cause another bank to pay, a fixed or determinable amount of money to a beneficiary if:
>
> (1) The instruction does not state a condition to payment to the beneficiary other than time of payment;
>
> (2) The receiving bank is to be reimbursed by debiting an account of, or otherwise receiving payment from, the sender; and
>
> (3) The instruction is transmitted by the sender directly to the receiving bank or to an agent, funds transfer system, or communication system for transmittal to the receiving bank.

Id.

[320] Baldwin, *supra* note 78, at 432.

[321] *See World's Laundering Laws Being Outpaced by Technology, U.S. Says*, 7 MONEY LAUNDERING ALERT 11 (April 1996) (stating that "'the money laundering problem confronting policymakers and enforcement agencies [is] becoming ever more complex and pervasive,' according to the annual U.S. State Department on the state of the world's money laundering and drug trafficking problems."); *see also id.* (stating that "[t]he benefits of using 'cybercurrency' to launder money surpass those of conventional currency" according to the International Narcotics control Strategy Report released in April of 1996); Sultzer, *supra* note 16, at 184 (stating that "[b]anks have, in effect, become the government's 'front line defense' in the fight against money laundering [and consequently] money laundering has moved out of the highly regulated world of mainstream banking."). The 1997 FATF Report notes that:

> [a]s regards money laundering techniques, the most noticeable trend is the continuing increase in the use by money launderers of non-bank financial institutions and non-financial businesses relative to banking institutions. This is believed to reflect the increased level of compliance by banks with anti-money laundering measures.

1997 FATF Report, *supra* note 4, ¶ 73.

sufficient safeguards in digital cash systems.[322] Citing the FATF report, a Group of Ten[323] Working Party[324] Report on Electronic Money also stressed that money laundering dangers created by electronic money systems necessitate close monitoring of this emerging technology to prevent any potential criminal activity.[325]

The most dangerous aspects of electronic money making it conducive to money laundering are its speed[326] and anonymity.[327] Fortified by cryptography, electronic money precludes re-

[322] 1997 FATF Report, *supra* note 4, ¶ 65. The FATF has noted that primary concerns raised by potential criminal use of digital money include:

> . . . (a) the need to review and potentially revise existing regulatory regimes to ensure adequate supervision of all types of e-money providers; (b) whether accurate and adequate records of transactions and persons involved will be available; (c) stored value cards may be more difficult to detect than physical currency; and (d) the speed and volume of e-money transactions may make it more difficult to track or identify unusual patterns of financial transactions.

Id.

[323] *See* Bruce S. Darringer, *Swaps, Banks, and Capital: An Analysis of Swap Risks and a Critical Assessment of the Basle Accord's Treatment of Swaps*, 16 U. PA. J. INT'L BUS. L. 259, 261 (1995) (stating that Group of Ten ("G-10") nations include Belgium, Canada, France, Germany, Italy, Japan, The Netherlands, Sweden, Switzerland, United Kingdom, and United States).

[324] *See* Group of Ten Report on Electronic Money, *supra* note 4, at 39 (noting that members of the Working Party include Belgium, Canada, France, Germany, Italy, Japan, Netherlands, Sweden, Switzerland, United Kingdom, United States, Bank for International Settlements, International Monetary Fund, European Commission, Organization for Economic Co-operation and Development, and European Monetary Institute).

[325] *Id.* at 12.

[326] *See* 1997 FATF Report, *supra* note 4, at ¶ 34 (stating that [t]he rapid movement of e-money . . . will make it difficult for law enforcement to identify or track these fund transfers."); Platts, *supra* note 13, at 8 (stating that "[t]he speed that makes [electronic money systems] efficient and the anonymity that makes it secure, make the system even more attractive to the launderer.").

[327] *See id.* at annex 1, ¶ 3 (stating that "[e]lectronic money (e-money) has the potential to make it easier for criminals to hide the source of their proceeds and move those proceeds without detection."); In addition to digital payment systems, banks operating on the Internet may also be exploited by criminals for money laundering purposes. *See* Hughes, *supra* note 13, at 1 (noting that, because Internet or "cyberspace" banks do not accept deposits and restrict their activities to acting as intermediaries in online purchases, they are not subject to federal or state regulation). *See also* Sultzer, *supra* note 16, at 195 (stating that "[c]yberbanks do not currently accept deposits; rather, they act as intermediaries in financial transactions and sales."); Sarah Jane Hughes, *"Phantom" Cyberbanks Pose Laundering, Tax Evasion Threat*, 6 MONEY LAUNDERING ALERT 4 (July 1995) (stating that "[t]he international consequences of cyberbanking are obvious . . . cyberbanks will permit the movement of billions of dollars across national boundaries annually."); Hughes, *supra* note 13, at 1 (noting that online money transfers facilitate money laundering because "[e]lectronic mail messages, aided by en-

tracing the countless transfers in the layering and placement stages of the laundering process.[328] Commentators warn that this problem will increase exponentially with the increased use of electronic wallets, which allow cross border person-to-person transfers of funds via telephone lines or computer networks.[329] Conducted outside the regulated network of financial institution, such transfers may thwart current measures enacted to prevent money laundering unless law enforcement officials can trace the funds without relying on paper trails.[330]

II. *THE KEY ESCROW DEBATE*

The French,[331] Russian,[332] and British[333] governments have

cryption and cyberspace banking transfers, will enable launderers to transfer assets around the world many times a day.").

[328] *See* Spernow, *supra* note 16, at 14 (stating that "[u]nbreakable encryption is the primary factor that puts CyberCrooks at an advantage over law enforcement . . . [c]urrent CyberCops agree and predict that there will be a substantial increase in cases where [they] were able to avoid prosecution because evidence that would have convicted them is encrypted and therefore unexaminable."); *see also* Sultzer, *supra* note 16, at 195 (noting that development of strong cryptography will enable cyberbanks to expand their money laundering activities).

[329] *See* Hughes, *supra* note 13, at 1 (stating that SVC technology enables individuals to move cash around the world via ATM); *see also* Sultzer, *supra* note 16, at 197 (noting ease with which electronic wallets are adopted for money laundering purposes because they enable transfer of money between over phone wires without intervention of banks).

[330] *See* Froomkin, *supra* note 29, at 477 (stating that "[if] digital cash that does not have to be cleared through a bank . . . becomes widespread, the ability of authorities to control money laundering will depend greatly on the extent to which the scheme allows authorities to trace the funds."); *see also G-10 Nations Chart Course for Cyberlaundering Controls*, 8 MONEY LAUNDERING ALERT 10, 11 (1997) (stating that "[t]he speed, anonymity and international nature of cyberpayments systems thwart the subjective evaluations required in suspicious activity reporting, which has become the focal point of global laundering controls.").

[331] *See* Froomkin, *supra* note 209, at 60 (noting that France currently has most developed cryptography regulations in Europe, and recently passed laws relaxing control over escrowed cryptography). The proposed amendment to the French Telecommunications Act of 1996 lays the foundation for establishing key escrow authorities:

> II - The bodies responsible for managing the secret keys pertaining to encryption devices and services which provide confidentiality, on behalf of third parties, shall be subject to prior approval from the Prime Minister.
>
> . . .
>
> A State Council decree shall define the conditions governing the approval of these organizations and shall set out the procedures and technical provisions required to implement [their obligations as set forth in the French Telecommunications Act].

French Key Escrow Regulation, *supra* note 18, art. 17.

[332] *See Russia Wants to Adopt Key Escrow*, IND. PUB. INT. NEWSLTR., Jan. 30, 1997

expressed an interest in establishing key escrow to fortify the interests of law enforcement in fighting electronic crime. Similar to the Clinton Administration's Clipper III[334] proposal, the British proposed key escrow system utilizes a network of trusted third parties to hold and manage private keys.[335] The European Community and United States disagree on the proper means to implement key escrow.[336] While EC officials have opined that key escrow should develop as a product of market forces, the United States supports aggressive implementation of key escrow authorities by individual governments.[337]

A. *European Community*

The Commission of the European Communities voiced its essentially negative opinion[338] of key escrow in an August 1997

(stating that Arkadi Golubkov, chairman of Russian Security Council's Committee for Computer Security, leads group of fifteen representatives of government departments in formulating regulations to implement cryptographic key escrow mechanism in Russia).

[333] *See UK: Encryption: The Debate Continues . . .*, REUTER TEXTLINE COMPUTING, June 5, 1997 (stating that "[a] public consultation paper, issued [in March of 1997 by the British government], proposes that all those who want to keep digital data private by encrypting it must first make sure the government has free and easy access to the software key which will scramble it."); *see also* British DTI Public Consultation Paper, *supra* note 17 (setting forth key escrow proposal).

[334] *See generally* White Paper, *supra* note 19 (proposing key escrow infrastructure administered by key certification authorities).

[335] *See generally*, British DTI Public Consultation Paper, *supra* note 17. The U.K. proposal states that:

> [l]egal access can be achieved by making use of a key escrow/recovery system. Key recovery allows authorized persons (for example users, officers of an organization and law enforcement authorities) under certain conditions, to decrypt messages with the help of cryptographic key information, held in escrow, and supplied by one or more trusted parties.' In such cases legal access is to the private confidentiality key.

Id. ¶ 37.

[336] *See* Brooks Tigner, *EU Aims to Spur Encryption Trade by Lifting Limits*, DEFENSE NEWS, Oct. 13, 1997, at 94 (comparing EC and U.S. key escrow policy).

[337] *Id.*

[338] *But see* Froomkin, *supra* note 209, at 61 (stating that EU has proposed project to establish European network of trusted third parties under control of member nations that resembles UK proposal). On the subject of cooperation with the EU, the British DTI Public Consultation Paper states that:

> It is recognized that complementary European Commission initiatives on Trusted Third Parties would be appropriate to enable an EU wide network of TTPs to be established. The Government has therefore, been working closely with the European Commission on the scope and content of applicable measures. The Government, in concert with other European countries, has recom-

Communication[339] in which it articulated Europe's future course of action regarding digital signatures and encryption.[340] Noting the debate surrounding regulation of cryptography in France, Great Britain, and the United States, the Commission presented three arguments against enacting a key escrow infrastructure.[341] These include inevitable vulnerability,[342] prohibitive cost,[343] and questionable effectiveness.[344] In conclusion, the Commission stated that economic well-being of industry involved in the development of electronic commerce takes precedence over any government-sponsored mandatory key escrow programs.[345]

At the European Ministerial Conference[346] on July of 1997, Ministers from the Member States of the European Union noted the great importance of encryption technology in protecting the

> mended that the Commission adopt measures to demonstrate, trial and pilot TTP projects which would underpin the EU wide development of encryption services through TTPs

British DTI Public Consultation Paper, *supra* note 17, ¶ 21.

[339] Communication on European Encryption Policy, *supra* note 23, COM (97) 503 Final.

[340] *Id.* at 2. The stated purpose of the Communication on European Encryption Policy includes:

> [e]nsuring the functioning of the Internal Market for cryptographic products and services as well as products ans services incorporating cryptographic techniques, while respecting public security concerns and contributing to a homogenous security area in the EU . . . .

Id. The Commission also proposed to enact a common European framework on cryptography in accordance with the objectives in the Communication by the year 2000. *Id.* at iii.

[341] *Id.* at 12-13.

[342] *See id.* at 13 (stating that "[i]nevitably, any key access scheme introduces additional ways to break into a cryptographic system").

[343] *See id.* (stating that "[t]he costs associated with key escrow can be very high [and], up to now, questions on costs and who would bear them have not been addressed by policy makers").

[344] *See id.* (stating that "[k]ey access schemes can be easily circumvented - even if, hypothetically speaking, everyone would be forced to pass through these systems").

[345] *Id.*

[346] GLOBAL INFORMATION NETWORKS MINISTERIAL DECLARATION NO. 20 (1997) [hereinafter MINISTERIAL DECLARATION]. Participants at the Conference included Ministers of the Member States of the European Union, members of the European Free Trade Association, members of the European Commission, officials from the United States, Canada, Japan, Russia, and representatives from industry. *Id.* at 1. The MINISTERIAL DECLARATION identifies the objective of the conference as "to broaden the common understanding of the use of Global Information Networks, to identify barriers to their use, to discuss possible solutions and to undertake an open dialogue on further possibilities for European and international co-operation." *Id.*

fragile developing electronic commerce.[347] The Ministers also noted the OECD[348] guidelines as a basis of future cryptography policy, and encouraged industry to lead the development of encryption.[349] The OECD Council Guidelines, published on March 27, 1997, identify eight general principles for nations to follow in order to successfully implement encryption and promote electronic commerce.[350] As part of the sixth principle, the

[347] *Id.* The MINISTERIAL DECLARATION notes that,

> Ministers recognize that advances in Global Information Networks have the potential to affect every aspect of our society - from commerce to health care, from education to leisure, from the practice of government to the exercise of democracy . . . . [T]hey note that the Internet is already starting to create new businesses, new high-value services, and, most importantly, new jobs . . . . Global Networks represent a powerful influence in the social, educational and cultural fields - empowering educators, lowering barriers to entry for the creation and dissemination of content in different languages, offsetting the effect of distance for more remote users and offering users access to ever richer sources of information . . . . Equally importantly . . . Global Information Networks give practical reality to freedom of expression and access to information.

Id. ¶¶ 2,4-5.

[348] MINISTERIAL DECLARATION, *supra* note 346, ¶ 36. The OECD, an acronym for Organization for Economic Cooperation and Development, is a coalition of nations formed to promote their mutual economic growth and the general expansion of world trade. OECD CHARTER art. 1. The OECD was created in 1961 to replace the post-war Marshall Plan's Organization for European Economic Cooperation ("OEEC"). *OECD Facing Identity Crisis*, JAPAN ECONOMIC NEWSWIRE, May 18, 1997. Based in Paris, the OECD is comprised of twenty nine member nations. Brian Love, *OECD Adopts Communications Encryption Guidelines*, REUTERS WORLD SERVICE, March 27, 1997. *See* Stewart A. Baker, *Decoding OECD Guidelines for Cryptography Policy*, 31 INT'L LAW. 729 (1997) (noting that OECD Member Nations include Austria, Australia, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, New Zealand, The Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States).

[349] MINISTERIAL DECLARATION, *supra* note 346, ¶ 37.

[350] Organization for Economic Cooperation and Development, *Recommendation of the Council Concerning Guidelines for Cryptographic Policy* (March 27, 1997) (visited July 29, 1997) <http://www.oecd.org/disti/iccp/crypto_e.html> (also on file with the *Fordham International Law Journal*) [hereinafter OECD Guidelines]. The eight principles articulated in the OECD Guidelines are:

1. Trust in cryptographic methods: Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems.
2. Choice of cryptographic methods: Users should have a right to choose any cryptographic method, subject to applicable law.
3. Market driven development of cryptographic methods: Cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments.

OECD urges that lawful access to cryptography should be developed in light of the other principles, which weigh heavily in favor of privacy and market-driven development of encryption technology.[351] Although the Guidelines are not binding on OECD member nations, they reflect the sentiments and likely future policy of the European Community regarding encryption and key escrow.[352]

B. *France*

Commentators have noted that France has the most comprehensive framework of cryptography regulations in the world.[353] The French government is currently considering a proposed regulation that authorizes the formation of key escrow agents to store cryptographic keys.[354] The regulation provides that escrow agents must disclose the keys to law enforcement authorities as otherwise required by the French Criminal Procedure Code.[355] The regulation also relaxes export restrictions on

4. Standards for cryptographic methods: Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at the national and international level.
5. Protection of privacy and personal data: The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.
6. Lawful Access: National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.
7. Liability: Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated.
8. International cooperation: Governments should cooperate to coordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade.

Id.

[351] *Id.*

[352] Love, *supra* note 348.

[353] *See id.* at 11-12 (stressing singular nature of French cryptography regulation, only one currently enacted in Europe); *but see* Froomkin, *supra* note 209, at 60 (noting that, although France has possibly most comprehensive cryptography laws in world, they are generally not enforced).

[354] *See* French Key Escrow Regulation, *supra* note 18, art. 17, § 2 (providing for creation of bodies for managing keys pertaining to encryption devices).

[355] *Id.* art. 17, § 2 (setting forth procedure for disclosing keys to legal authorities under chapters I and II of book I of French Criminal Procedure Code).

escrowed encryption.[356]

C. *Great Britain*

In June of 1996, Ian Taylor, Britain's Minister for Science and Technology, announced an upcoming Consultation Paper on the British Government's proposals for regulation of cryptographic keys.[357] The Consultation Paper, entitled Licensing of Trusted Third Parties for the Provision of Encryption Services, was issued by the British Department of Trade and Industry ("DTI") in March of 1997.[358] The DTI introduces the proposal by stressing that, as the need to secure electronic commerce creates greater need for cryptography, the more widespread use of cryptography itself will create new dangers for law enforcement by allowing criminals to obfuscate their illegal activities.[359] Because of this, the Consultation Paper states that government must have access to appropriate mechanisms to decrypt suspect transmissions.[360]

The Consultation Paper outlines a plan for the provision of a network of trusted third parties[361] ("TTPs") which would serve as the government's storehouses of private keys to be released pursuant to a warrant.[362] Noting the international scope of electronic commerce, the Consultation Paper stresses that the TTP network should extend across national borders.[363] Allowing for licensing of domestic issuers of cryptography with foreign TTPs, it also underscores the need to establish similar standards in all nations supporting the TTP network.[364]

[356] *Id.* art. 17, § 1(b); *see* Froomkin, *supra* note 209, at 60 (discussing French government plan to relax export controls in return for compliance with escrow laws).

[357] British DTI Public Consultation Paper, *supra* note 17 (introductory comments of Ian Taylor).

[358] *Id.*

[359] *See id.* ¶ 36 (stating that "[a] critical issue presented by cryptography is the possible conflict between privacy and law enforcement").

[360] *See id.* ¶ 38 (adding that securing law enforcement interests through key escrow would permit government to relax current export controls on strong cryptography).

[361] *See* Froomkin, *supra* note 203, at 55 (describing function of trusted third parties as storing cryptographic keys and certifying identity of key users).

[362] British DTI Public Consultation Paper, *supra* note 17, ¶ 46. The Consultation Paper's mandatory key escrow provisions exclude organizations providing encryption services to their employees for intra-company use only and encryption used as part of another service such as encoding digital cable transmissions. *Id.* ¶¶ 48-49.

[363] *Id.* ¶ 18.

[364] *Id.* ¶ 21. In support of its proposal for an international TTP network, the DTI

In addition to serving as key escrow agents, TTPs would also provide necessary services such as authentication of digital signatures and recovery of lost or corrupted keys, thus facilitating electronic trade in general.[365] Although the Consultation Paper mandates that all providers of encryption technology must obtain a license, subscribers to such services need not use TTPs.[366] Thus, whereas market forces would drive the assimilation of TTPs into electronic commerce, government would have access to encryption regardless of their acceptance.[367] Among the general benefits of TTPs, the Consultation Paper lists greater protection of the consumer, more widespread access to encryption technology, secure electronic trading, and easier data recovery.[368] Opponents of the Consultation Paper point out, however, that keys stored by TTPs are vulnerable to theft and use by the British government for industrial espionage.[369] Others attack it by noting that unescrowed black market cryptography will emasculate the government's ability to decrypt transmissions with escrowed keys.[370]

D. *United States*

In 1994, the National Security Agency published the Escrowed Encryption Standard[371] ("EES") hoping to establish the

Public Consultation Paper cites the OECD Cryptography Guidelines, which stressed the need for international cooperation in formulating uniform standards for encryption. *Id.* ¶ 23.

[365] *Id.* ¶ 39.

[366] *Id.* ¶ 45.

[367] *See id.* at annex F (stating that "[t]he market will decide if it wants to use TTP services [and those] wishing to do otherwise will be at liberty to do so.").

[368] *Id.* ¶ 42.

[369] *See UK: Encryption-The Debate Continues*, REUTER TEXTLINE, COMPUTING, June 5, 1997, at 25 (discussing opposition to British DTI Public Consultation Paper).

[370] *Id. Cf.* British DTI Public Consultation Paper, *supra* note 17, Annex F (stressing that despite criminal's ability to circumvent key escrow through unlicensed encryption technology, government can at minimum access electronic transmissions to the extent that licensed TTP services are used by public).

[371] *Cf.* Amy Fleischman, *Personal Data Security: Divergent Standards in the European Union and the United States*, 19 FORDHAM INT'L L.J. 143, 177 (1995) (stating that "[t]he U.S. Government's continued ability to eavesdrop on data communication encrypted with the [escrowed encryption standard] will render this encryption system incompatible with [Article 17 of European Parliament's Directive 95/46/EC, and] EU member states . . . will continue to prohibit data communications encrypted with key escrow technology from entering their jurisdictions."). The European Parliament Directive 95/46/EC which prohibits member states to transmit individuals' personal data to countries having relaxed data protection laws, may be interpreted as standing opposed

U.S. government's authority to access encrypted transmissions.[372] The standard created what became known as the Skipjack, a classified algorithm using an eighty bit symmetric key.[373] The U.S. government incorporated this standard into the Clipper[374] chip, which enabled users to encrypt telephone conversations, and the Capstone Fortezza PCMCIA card, used for e-mail and computer file encryption.[375] The Clipper and Capstone chips were made available for purchase by the public.[376] The U.S. government, however, retained copies of the cryptographic keys to each manufactured chip, allowing it to intercept and decrypt any message sent using the Skipjack technology.[377]

Although the Capstone chip gained some popularity,[378] the Clipper chip was vehemently rejected by the public.[379] In response, the Clinton administration launched a second proposal called Clipper II.[380] The new proposal allowed an exception to

to key escrow. *See* Parliament and Council Directive No. 95/46, art 25, O.J. L 281/31, at 45 (1995) (prohibiting Member States from transferring personal data to countries not having adequate levels of protection for such data). However, the Directive does not apply to laws enacted to prevent financial crime. *See* Group of Ten Report on Electronic Money, *supra* note 4, at n.10 (stating that "[Directive 95/46/EC] is not applicable to national legislation aimed at preventing, investigating and prosecuting criminal activity affecting the payment system."). Furthermore, the European Council expressly recognized the primacy of law enforcement interests over personal privacy in its Resolution on the Lawful Interception of Telecommunications. Council Resolution of 17 January 1995, O.J. C 329/1, at 1 (1995) (noting that Resolution requirements for lawful interception of telecommunications constitute important conditions for effective law enforcement in modern telecommunications systems).

[372] Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES), 59 Fed. Reg. 5,997 (Feb. 9, 1994).

[373] *See* Froomkin, *supra* note 209, at 23-24 (explaining policy behind Skipjack and its operation).

[374] *Id.* at 23. The name "Clipper" refers to the encryption system set forth in the EES. *Id. See also* Froomkin, *supra* note 29, at 502 (stating that "[t]he government's right to access the information in this 'Clipperized cash' could be hedged with procedural safeguards, or it could be triggered automatically whenever a Clipperized digital cash transaction exceeded current reporting limits.").

[375] Froomkin, *supra* note 209, at 24.

[376] *Id.*

[377] *Id.*

[378] *See id.* at 32 (stating that "Capstone . . . has had at least some success, albeit not enough to achieve the FBI's goal of ensuring that cryptography imposes no obstacles to law enforcement's legal efforts to acquire the content of electronic communications and stored data.").

[379] *See* Robyn Blumner, *Under Clinton, Government Is All Ears*, COMM. APPEAL, Aug. 11, 1996, at B5 (arguing that Clipper proposal needlessly invades users' privacy).

[380] Field, *supra* note 55, at 993.

export restrictions[381] on cryptographic algorithms and keys of up to sixty-four bits provided that the keys were deposited with a government-approved escrow mechanism.[382] Clipper II met significant opposition from U.S. hardware and software manufacturers who claimed that the lack of similar export controls in other nations needlessly impaired sales overseas.[383] In May of 1996, the Clinton administration proposed Clipper III in a government White Paper entitled Enabling Privacy, Commerce, Security, and Public Safety in the Global Information Infrastructure.[384] In the White Paper, the Clinton Administration proposed the creation of a worldwide Key Management Infrastructure ("KMI"), eliminating the need for export controls.[385] In a public statement on October 1, 1996, Vice Presi-

[381] *See* Kerben, *supra* note 15, at 130 (noting that, until October 1, 1996, U.S. government considered cryptography munition under Arms Control Export Act, 22 U.S.C. § 2778 subject to International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. § 120). Under the ITAR, the Department of State must grant permission allowing export of software encryption products with keys longer than 40 bits. 22 C.F.R. § 120. On October 1, 1996, President Clinton signed executive order 13026, 61 Fed. Reg. 58,767, which vested the Commerce Department with authority to regulate cryptography. Kerben, *supra* note 15, at 130. The Commerce Department's Export Administration Regulations define cryptography as dual-use technology, having both commercial and military applications. 15 C.F.R. § 772; Kerben, *supra* note 15, at 131.

[382] *See* Dorothy E. Denning, William E. Baugh, Jr., *Symposium: Recent Developments: Key Escrow Encryption Policies and Technologies*, 41 VILL. L. REV. 289, 291 (discussing Clipper II proposal).

[383] *See* Froomkin, *supra* note 209, at 41 (stating that businesses wishing to export products involving cryptographic technology "did not think the [export control] rules would allow them to export a commercially viable product."); *see also* Kerben, *supra* note 15, at 134 (stating that one could have purchased U.S. export-restricted encryption program in Russia for about five dollars); *id.* (noting that despite U.S. export controls, individuals around world could have downloaded encryption programs from Internet which could not be exported from United States under existing regulations).

[384] White Paper, *supra* note 19.

[385] *Id.* The White Paper sets forth the following principles:

- Participation in the KMI will be voluntary. Key escrow in the KMI will occur naturally through mutually trusted authorities;
- There will be a transition period during which legacy equipments which do not support key recovery can be used to communicate with users in emerging full featured KMIs. (Government, industry, and users will need to address the legitimate needs of those currently using non-key recovery products to communicate with users of the full-featured KMI in a manner that protects legitimate government and public safety concerns. This will provide a transition path.);
- Products that operate with an escrowed KMI need to be developed with the industry taking the lead;
- Industry can continue to lead in establishing standards for public key certificates, encryption algorithms, protocols, data recovery, and security services;

dent Al Gore presented Clipper IV, allowing the export of cryptography using up to fifty-six bit keys for two years provided that industry cooperates by incorporating key recovery features into future products.[386]

III. *THE EUROPEAN COMMUNITY SHOULD ALIGN ITS EFFORT WITH GREAT BRITAIN, FRANCE, AND THE UNITED STATES TO DEVELOP A JOINT NETWORK OF KEY ESCROW AGENCIES IN ORDER TO PREVENT THE USE OF DIGITAL PAYMENT SYSTEMS FOR MONEY LAUNDERING PURPOSES*

The European Commission wrongly rejects key escrow as unworkable and harmful to electronic commerce.[387] By giving law enforcement authorities access to encrypted electronic transmissions, key escrow authorities represent the primary tool for detecting and eliminating digital money laundering.[388] Nations should not stand idly by while criminals find ways to hide illicit funds with encryption.[389] Unless regulated, cryptography will allow money launderers to obfuscate the complicated trail of digital transfers conducted to associate money with legitimate sources.[390]

A. *Traditional Money Laundering Control Measures Will Fail to Prevent Electronic Money Laundering.*

Existing laws enacted to prevent money laundering do not consider the implications of digital money and thus will fail to

- Self-escrow will be permitted under specific circumstances; and
- Export controls on Key Escrow products will be relaxed progressively as the infrastructure matures.

Id.

[386] *See* Gore Speech, *supra* note 19 (stating that "under this initiative, the export of fifty-six bit key length encryption products will be permitted under a general license after one-time review and contingent upon industry commitment to build and market future products that support key recovery.").

[387] *See supra* notes 338-52 and accompanying text (discussing European Community's opposition to government-sponsored key escrow).

[388] *See supra* notes 252-56 and accompanying text (discussing benefits of key escrow in preventing crime and facilitating electronic commerce).

[389] *See supra* notes 321-30 and accompanying text (discussing adaptability of digital payment systems for money laundering purposes).

[390] *See supra* notes 215-29 and accompanying text (discussing importance of cryptography in digital payment systems); *see also supra* notes 230-45 and accompanying text (explaining difficulty of cracking cryptographic code).

prevent money laundering through digital payment systems.[391] Traditional money laundering laws focus on financial institutions which often serve as conduits for transferring illicit funds to legitimate businesses and accounts.[392] Once apportioned into smaller amounts and distributed among non-criminal sources, the money is easily funneled back into the criminals' hands.[393] To prevent this, laws such as the U.S. Bank Secrecy Act require financial institutions to document large transactions and report any suspicious activity.[394] Like many similar money laundering laws, the Bank Secrecy Act requires institutions to create a paper trail behind money transfers that law enforcement authorities can trace in the course of an investigation.[395] International agreements for combating money laundering also rely on financial institutions.[396] Such agreements typically require nations to provide foreign investigators with access to paper trails maintained by their domestic financial institutions.[397]

By enabling individuals to transfer money without using financial institutions, digital payment systems eliminate the effectiveness of laws that establish paper trails.[398] Money transferred from a bank account onto an SVC at an ATM or through an electronic wallet connected to a personal computer can be transferred anywhere in the world without a single reporting requirement.[399] This capability will allow money launderers to conduct

[391] *See supra* notes 275-320 and accompanying text (setting forth domestic and international initiatives that rely primarily on financial institutions to uncover evidence of money laundering).

[392] *Id. See also supra* notes 266-69 and accompanying text (describing placement and layering stages of money laundering where money is transferred between legitimate concerns to hide its source).

[393] *See, e.g., supra* note 270 and accompanying text (describing how BCCI helped money launderers reintegrate laundered money through legitimate transactions).

[394] *See supra* notes 302-05 and accompanying text (discussing BSA provisions requiring individuals and financial institutions to report money transfers).

[395] *See supra* note 302 and accompanying text (discussing currency transaction report mandated by BSA which served as paper trail facilitating investigations).

[396] *See supra* notes 275-98 and accompanying text (discussing international initiatives for combating money laundering).

[397] *See, e.g., supra* note 295 (setting forth provisions of Council Directive 91/308 requiring that Member States "shall ensure that credit and financial institutions . . . [e]stablish adequate procedures of internal control and communication in order to forestall and prevent operations related to money laundering.").

[398] *See supra* notes 116-17 and accompanying text (describing operation of electronic wallets which enable individuals to transfer money without using regulated financial institutions).

[399] *Id.*

countless amounts of transfers for purposes of layering illicit funds.[400] Although law enforcement authorities can intercept these electronic transmissions, cryptography prevents them from deciphering their content.[401] Controlling digital money laundering therefore translates into having access to encrypted communications.[402]

B. *In Order to Effectively Police Digital Payment Systems, Law Enforcement Authorities Must Have Access to Cryptographic Keys*

Cryptography presents an insurmountable barrier to tracing suspect electronic transmissions.[403] Without access to the content of ciphertext,[404] law enforcement authorities cannot determine the transmission's origin, destination, or whether it includes digital money.[405] Access to encrypted data depends on finding the correct decryption key.[406] This, however, may take years for even the most powerful computers.[407] In order to effectively trace illicit funds structured in the money laundering process within sufficient time to convict the responsible parties, law enforcement authorities should have the capability to decrypt electronic transmissions.[408] Governments can secure this capability by establishing escrow agencies to hold copies of active cryptographic keys.[409] An international network of key escrow agencies would provide investigators with a quick and easy mech-

[400] *See supra* note 4 (noting commentators' warning regarding adaptability of digital payment systems for money laundering purposes).

[401] *See supra* notes 230-45 and accompanying text (describing difficulty in finding symmetric and asymmetric keys).

[402] *See supra* note 35 (noting legal authorities' concern about difficulty of policing encrypted communications).

[403] *See supra* notes 230-46 and accompanying text (describing arduous process of cracking cryptographic codes).

[404] *See supra* notes 176-84 and accompanying text (explaining formation of symmetric ciphertext).

[405] *See supra* notes 15-16 and accompanying text (describing barriers to effective law enforcement caused by use of cryptography to encode electronic transmissions).

[406] *See, e.g., supra* notes 233-46 and accompanying text (discussing methods of finding symmetric and asymmetric keys); *see also supra* notes 215-29 and accompanying text (describing the role of cryptography in mechanics of digital money).

[407] *See* Kerben, *supra* note 15, at 129 (noting recent study finding that, in order to crack 1024 bit key, one would need one hundred million computers with eight Megabytes of RAM operating at 100 MHZ for 280,000 years).

[408] *See supra* note 330 (noting experts' opinion that cryptography will complicate tracing laundered money).

[409] *See supra* notes 246-56 and accompanying text (discussing operation of key escrow agents).

anism to investigate suspect transmissions,[410] and thus effectively eliminate the conscription of digital payment systems for money laundering purposes.

C. *The European Commission's Reasons for Opposing the Creation of Key Escrow Agencies Lack Factual Support*

In its August 1997 Communication, the European Commission opposed vesting governments with the authority to aggressively develop key escrow networks.[411] First, the Commission claimed that any key escrow system would inevitably fall prey to computer-literate criminals.[412] Although this may likely happen on a small scale, legal authorities in the United States and Great Britain have pointed out that taking no precautionary measures against the potential criminal use of encryption will create insufferable future problems.[413] If governments act too late in establishing safeguards, the technological tide may uncover even greater barriers to prosecuting money launderers. Although today's computers, for example, can decode encrypted transmissions, the development of longer cryptographic keys may soon eliminate this capability.[414]

The Commission also proposed that the cost of establishing key escrow, both in terms of monetary expenditure and restraint on electronic commerce, renders it improper for achieving its purported aim.[415] This argument fails to consider that key escrow presents significant economic benefits. For example, as

[410] *See, e.g.*, *supra* notes 359-60 and accompanying text (noting necessity of key escrow agencies to law enforcement stressed by British DTI Public Consultation Paper).

[411] *See supra* notes 338-45 and accompanying text (noting Commission's argument that implementation of key escrow would suffer from inevitable vulnerability, prohibitive cost, and low effectiveness).

[412] *See supra* note 342 (citing Commission statement that "[i]nevitably, any key access scheme introduces additional ways to break into a cryptographic system.").

[413] *See supra* notes 359-60 and accompanying text (noting British Government's concern about unregulated proliferation of cryptography); CRISIS REPORT, *supra* note 5, at 170 (warning that failure to implement key escrow may result in "proliferation of products with encryption capabilities that would seriously weaken, if not wholly negate, the authority to wiretap . . . and damage intelligence collection for national security and foreign policy reasons.").

[414] *See supra* note 238 (noting possible development of cryptographic keys of sufficient length to place technological requirements for breaking code outside limits of physical science).

[415] *See supra* note 343 (citing Commission's statement that "[t]he costs associated with key escrow can be very high [and], up to now, questions on costs and who would bear them have not been addressed by policy makers.").

pointed out by the U.S. Clipper II, III, and IV proposals, key escrow will facilitate the general oversight of encrypted data and thus eliminate the need for export controls on escrowed encryption.[416] This, in turn, would drive the market for strong cryptography and ultimately result in safer and thus more robust electronic commerce. In addition, the British DTI Public Consultation Paper proposes using key escrow agencies as providers of consumer services such as recovery of lost keys and authentication of digital signatures.[417] Such services are indispensable to electronic commerce,[418] and would generate substantial fees that could be used to maintain the key escrow infrastructure.

D. *Proposal*

The proper means of implementing an international key escrow network should include both aggressive legislation and economic incentives for the participants. The Commission incorrectly concludes that the market should play the primary role in developing key escrow agencies. The market, in fact, has proven that the lucrative practice of money laundering attracts many legitimate businesses.[419] Governments, therefore, should pursue legal access to encrypted data despite opposition from industry. By establishing key escrow agencies that can also authenticate digital signatures and re-issue lost keys, governments will reap support from the expanding market for services supporting electronic commerce.[420]

Most importantly, key escrow must be the product of international cooperation. Current multilateral agreements echo the widespread realization that money laundering can only be fought effectively if criminals have relatively few safe harbors to

[416] *See supra* notes 380-86 and accompanying text (discussing Clipper II, III, and IV policy of permitting export of cryptography in exchange for industry cooperation in creation of key escrow infrastructure); *see also* note 383 and accompanying text (noting dissatisfaction of U.S. computer industry resulting from export controls on cryptography which adversely impacted overseas sales).

[417] *See supra* notes 365-70 and accompanying text (setting forth suggestions of British DTI Public Consultation Paper to employ key escrow agencies as providers of various consumer services).

[418] *See, e.g., supra* notes 203-14 and accompanying text (discussing mechanics of digital signatures and their role in electronic commerce).

[419] *See supra* notes 270-74 and accompanying text (describing money laundering process).

[420] *See supra* notes 211-14 and accompanying text (discussing need for certification authorities for proper implementation of digital signatures).

hide illicit funds.[421] For example, Council Directive 91/308 notes that measures enacted to prevent money laundering will fail without international cooperation.[422] In addition, the Council of Europe Convention stresses the need for nations to minimize the adverse impact of bank secrecy laws on the detection of laundered money.[423] As these agreements suggest, divergent key escrow standards will allow money launderers to simply shift operations to countries with relaxed cryptography regulations. Future efforts to prevent money laundering should build upon international cooperation which has proven effective in past initiatives.

CONCLUSION

Digital money represents the future of commerce and banking. Along with its many benefits, however, it brings daunting concerns for law enforcement authorities. By allowing individuals to transfer money quickly and anonymously without triggering any reporting requirements, digital payment systems provide the ideal mechanism for laundering money. Key escrow agencies can provide a necessary solution to this impending problem by furnishing law enforcement authorities with cryptographic keys to decode suspicious electronic transmissions within sufficient time to detect and convict money launderers.

[421] *See generally supra* notes 275-98 and accompanying text (discussing multilateral initiatives calling for nations' cooperation in combating money laundering).

[422] *See supra* notes 288-95 and accompanying text (discussing purpose and provisions of Council Directive 91/308).

[423] *See supra* note 287 (citing Article 4 of Council of Europe Convention mandating that "[e]ach party shall adopt such legislative and other measures as may be necessary to empower its courts or other competent authorities to order that bank, financial or commercial records be made available to be seized in order to carry out [law enforcement].").