Harvard Journal of Law & Technology
Volume 11, Number 3 Summer 1998

TO REGULATE OR NOT? MANAGING THE RISKS OF E-MONEY AND ITS POTENTIAL APPLICATION IN MONEY LAUNDERING SCHEMES

Timothy H. Ehrlich[*]

INTRODUCTION

Consider the situation of a drug kingpin in control of a large narcotics organization. Inevitably, he[1] would be faced with the question of how to convert the loads of low denomination, "dirty" paper bills (i.e., collected from street sales) into a form that could be easily moved. In addition, he would want to be able to transfer these funds to suppliers and his own bank accounts without revealing the source of the funds to law enforcement agencies. One option criminals often pursue in this situation is to "launder" money. This might involve placing the money into a bank or investment account in the United States and transferring it by wire to criminal accounts all over the world. Alternatively, one might choose to avoid dealing with U.S. financial institutions altogether by loading the money into cargo containers or suitcases and sending them out to foreign countries on ships or commercial airlines, respectively.

Interestingly enough, money laundering schemes such as these operated with impunity from the early part of this century up until the late 1970s.[2] Over the last few decades, however, U.S. law enforcement has been somewhat more successful in stopping money laundering activities.[3] In particular, this has resulted from the enactment of federal legislation aimed at preventing money laundering through U.S. banks, enhancing security measures at border stations and ports, and advancing surveillance technologies.[4] And yet, despite these efforts, it is still

---

* J.D., Class of 1999, Harvard Law School.

1. This paper uses the pronoun "he" for simplicity although the people exemplified could also be women.

2. *See* PRESIDENT'S COMMISSION ON ORGANIZED CRIME, THE CASH CONNECTION: ORGANIZED CRIME, FINANCIAL INSTITUTIONS, AND MONEY LAUNDERING 9, 17 (1984).

3. *See Bank Admits Money-Laundering*, STAR-TRIB., Nov. 3, 1990, at A10; Nilo Geyelin & David Finkel, *Bank Indicted on Drug Money Charge*, ST. PETERSBURG TIMES, Oct. 12, 1988, at A1; William Polk, *Money Changer Indicted in Laundering Case*, SAN DIEGO UNION-TRIB., Dec. 18, 1985, at B1.

4. Indeed, the Financial Action Task Force ("FATF"), an intergovernmental research body, recently stated that as bank regulations have gotten more effective, the

widely recognized that countless sums of money are laundered successfully through financial institutions all over the world every year.[5] Consequently, money laundering still represents a serious problem for the United States specifically and law enforcement in general.

Now imagine what would happen if certain advances in technology permitted the same criminal to transmit his criminal proceeds directly, instantaneously, anonymously, and globally without an audit trail and without resorting to a traditional financial institution (i.e., a bank). What if he could just load a million dollars from his U.S. bank account onto an untraceable plastic card, slip the card into his wallet, and board a plane to an offshore banking haven to unload the value? The current supervisory roadblocks and investigative techniques set up to stop more conventional types of money laundering would be useless. Unfortunately, the development of various electronic money systems holds the potential to make these scenarios a frightening reality in the very near future.

Designed as efficient and convenient payment systems for consumer transactions, electronic money systems currently exist in either card-based or software-based forms. Although many of these products are still relatively untested in the global consumer markets, it is already possible to recognize some general features of these systems that, if unchecked, may offer sizable advantages to money laundering organizations or individuals seeking to avoid detection within the United States. Consequently, these features could pose a significant threat to U.S. law enforcement efforts. Despite the imminence of this threat, the U.S. government has not taken reasonable steps to prepare, preferring instead to study the issues exhaustively.

This paper will argue that the federal government's approach to the regulation of electronic money systems within the United States is misguided and potentially harmful to the American economy. Moreover, this paper proposes an alternative system that more

---

amount of illegal funds being funneled through the traditional banking sector has decreased dramatically. *See* FINANCIAL ACTION TASK FORCE, FINANCIAL ACTION TASK FORCE REPORT ON MONEY LAUNDERING para. 25 (1997) [hereinafter FATF REPORT], *available at* <http://www.usis-israel.org.il/publish/press/global/archive/1997/march/gi703311.htm>.

5. Due to the fact that, by its nature, a successful money laundering scheme is not detected by a supervisory agency, one can estimate the amounts being laundered only by extrapolating outward from the amounts seized. For example, the 1997 FATF Report showed that one law enforcement agency prosecuted over 1,233 cases of money laundering between October 1995 and August 1996, with a total value of $1.62 billion. *See id.* para. 8. In Australia, officials projected the amount of money laundered in their country during 1995 to be approximately USD $2.8 billion. *See id.* para. 6.

adequately addresses the concerns and interests of the electronic money industry, its consumers, and U.S. law enforcement agencies. To that end, Parts I and II introduce the basic problem of how traditional methods of combating money laundering in the United States may soon be rendered useless by the advent of electronic money technologies. Part III critiques the federal government's current approach to these potential problems and Part IV provides a detailed alternative framework for the immediate regulation of electronic money systems in the United States. Finally, Part V evaluates the positives and negatives of this alternative approach.[6]

I. THE FUNDAMENTALS OF MONEY LAUNDERING AND U.S. EFFORTS TO STOP IT

A. The Basic Process of Money Laundering

Any systematic description of money laundering suffers from generalization because there is no limit to the creativity of the criminal mind. However, definitions from scholars and government agencies focus on the process by which drug traffickers and organized crime families have sought to make criminal proceeds appear legitimate by concealing their true amount, source, or application.[7] The laundering process has three parts: (1) "placement" — the initial entry of illicit funds into the stream of commerce; (2) "layering" — the subsequent transactions that conceal the true source of the funds; and (3) "integration" — the repatriation of money into the economy in disguised form.[8] After criminals "launder" their money, they use it to conduct their operations without suspicion from law enforcement agencies.

While it is difficult to generalize the types of schemes used by criminal organizations and individuals to launder their funds, there are strong patterns. One of the most common involves the use of financial institutions for the initial placement of funds. Illicit cash collected from

---

6. This paper addresses the specific effects that emerging electronic money technologies may have on traditional efforts to combat money laundering in the United States. This issue represents only a small part of the current debate surrounding electronic money. For that reason, several important issues, such as the international component of electronic money regulation, fall outside the scope of this analysis.

7. *See* EUGENE F. SMITH, MONEY LAUNDERING: A STUDY IN THE CREATION OF LAW 2 (1990).

8. *See Money Laundering and the Drug Trade: Hearings Before the Subcomm. on Crime of the House Comm. on the Judiciary*, 105th Cong., at sec. II (1997) (testimony of Michael F. Zeldin, Principal, Price Waterhouse), *available in* 1997 WL 416667.

street sales is delivered to a "bank house" or "safe house" controlled by the criminal organization. Once the cash has accumulated, it is delivered to a broker who distributes it to multiple import/export businesses. The broker uses wire transfers for the deposits and structures the amounts so as to fall below any bank reporting threshold (normally $10,000).[9] Next, the businesses would deposit the cash into banks under their corporate names and withdraw the same funds in the form of checks. With the checks, they purchase easily marketed, high-demand retail items, then export and resell them at below-market prices.[10] The proceeds from the sales are subsequently funneled back into the continued operations of the criminal organization.

Initially, criminals successfully laundered money through large American banks. However, the passage of bank reporting legislation in the 1980s, which will be discussed in more detail below, made it harder to launder funds through these institutions. In the United States and many other countries, little or no effort was made to subject non-bank financial institutions to the same kinds of regulations as banks. Consequently, launderers often wound up transferring their attention to brokerage houses and, later, non-bank financial institutions such as money exchangers, electronic funds transmitters and check cashiers.[11] Today, these types of financial institutions pose a very significant money laundering threat.[12] For example, a Mexican money exchange on the southwest border of the United States could accept cash from launderers south of the border and deposit it in U.S. commercial banks without having to identifying its customers. This money could then be deposited into other U.S. banks or invested without the intermediary bank ever learning the true source behind the funds.[13]

Other common examples of money laundering schemes involve the use of "shell" companies, which may exist only in the legal sense. Typically these companies are purchased "off the shelf from lawyers, accountants or secretarial companies"[14] and set up in the manufacturing industries to buy and sell goods for a profit. According to the FATF Report, this type of corporation benefits money launderers in that it

---

9. Law enforcement officials commonly refer to this technique as "smurfing." *See* FATF REPORT, *supra* note 4, at para. 16.

10. *See Money Laundering and the Drug Trade*, *supra* note 8, sec. II.A.

11. *See* FATF REPORT, *supra* note 4, at paras. 13, 25–29.

12. For example, in 1997, several FATF-member countries reported significant increases in the number of actual or suspected money laundering cases involving non-bank financial institutions. *See* FATF REPORT, *supra* note 4, at para. 26.

13. *See Money Laundering and the Drug Trade*, *supra* note 8, sec. II.F.

14. FATF REPORT, *supra* note 4, para. 18.

conceals the identity of the owner of the funds. The company records also are often harder to get at because they are offshore or held by professionals who claim secrecy, and the professionals typically act on instructions given to them by anonymous sources.[15] Equally significant, however, is the way in which they provide legitimization for the funds channeled through them.

Analogous to these schemes are ones involving real companies run by the criminals that are involved in phony business deals with inflated prices. Alternatively, some drug cartels use a parallel transaction to achieve the same result. According to Michael Zeldin, a principal of Price Waterhouse, a cartel using this scheme has their intermediary offer to pay directly, in dollars, for the cost of goods that a Colombian company plans to import from the United States.[16] Once the goods arrive in Columbia, the importers would pay the cartel for the goods with pesos, at slightly less than the going exchange rate. Given the high profit margins of the drug trade, this scheme is able to provide both a profit incentive for the company (which is now able to import its goods from the U.S. at substantially less cost) and an effective, anonymous means of laundering money for the cartel.

B. The Current Regulatory Scheme Established to Combat Money Laundering in the United States

To prevent and detect illegal movements of funds, law enforcement and regulatory officials have historically relied upon the intermediation of banks and other types of financial institutions.[17] These entities are viewed as providing "choke points"[18] through which illegal funds must generally pass, and thus, as a place where records of transaction and customer identities may be maintained.[19] The basic provision enacted by the United States to establish the legal framework for this type of system is the Bank Secrecy Act ("BSA").[20] Enacted in 1970, the BSA requires mandatory disclosure of information regarding large currency transactions, for various types of financial institutions. In essence, the act seeks to protect against laundering by creating a "paper trail"

---

15. *See id.*

16. *See Money Laundering and the Drug Trade*, *supra* note 8, sec. II.B.

17. *See* FATF REPORT, *supra* note 4, annex at para. 17.

18. *Id.*

19. *See* GROUP OF TEN, ELECTRIC MONEY: CONSUMER PROTECTION, LAW ENFORCEMENT, SUPERVISORY AND CROSS BORDER ISSUES; REP. OF THE WORKING PARTY ON ELECTRIC MONEY 15 (Apr. 1997).

20. 12 U.S.C. §§ 1951–1959, 31 U.S.C. §§ 321[illegible]11–5314, 5316–5322 (1994).

enabling investigators to trace illegal proceeds back to their sources.[21] Moreover, it provides for the Secretary of the Treasury to establish specific regulations aimed at catching money launderers, and places the Treasury Department solely in charge of monitoring and investigating compliance.[22]

The primary tools established in the regulations by the Secretary to track illegal funds are mandatory recording and reporting requirements. In particular, 31 U.S.C. § 5313 requires "financial institutions"[23] to file Currency Transaction Reports ("CTR"), which are records of any transaction greater than $10,000.[24] This requirement applies to banks, securities brokers, currency exchange houses, check cashiers, and individuals. Similarly, individuals must file a Report of International Transportation of Currency or Monetary Instruments ("CMIR") whenever they send more than $10,000 either into or out of the United States in any manner.[25] A Report of Foreign Bank and Financial Accounts ("FBAR") must also be filed if one has some tie to an account in foreign countries and the aggregate value of the accounts exceeds $10,000.[26] Finally, the regulations also impose specific customer identification requirements for financial institutions whenever they conduct a reportable transaction and before the transaction is completed.[27] Specifically, the institution must verify and record the name and address of the person conducting the transaction and record the identity, account number, and social security number of the person on behalf of whom the transaction is carried out.[28]

Following the creation of these requirements, several other legal developments helped to solidify the framework protecting against money laundering in the United States. In 1986, Congress passed the Money Laundering Control Act ("MLCA"), which essentially amended the BSA and made strategic structuring of transactions a crime. This was largely in response to the U.S. Court of Appeals for the First Circuit's decision in *United States v. Anzalone*,[29] which held that "structuring" a transaction in order to avoid bank filing requirements was not illegal

---

21. *See Money Laundering and the Drug Trade*, *supra* note 8, sec. III.1.
22. 31 U.S.C.§ 5313(a) (1994).
23. *See id.* § 5312.
24. *See* 31 C.F.R. § 103.2 (1996).
25. *See* 31 U.S.C. § 5316 (1994).
26. *See* 31 C.F.R. § 103.25 (1996).
27. *See* 31 C.F.R. § 103.28 (1996)
28. *See id.*
29. 766 F.2d 676 (1st Cir. 1985).

under 18 U.S.C. § 1001.[30] The MLCA also created two new categories of money laundering in sections 1956 and 1957.[31] Also included in the legal framework for laundering is the Trade and Business Reporting Act ("TBRA"),[32] enacted in 1984 as part of the Deficit Reduction Act of the Internal Revenue Code. Similar in effect to some of the other legislative safeguards, the TBRA requires trades and businesses to report cash and certain monetary instrument receipts to the IRS when they total more than $10,000. In addition, the TBRA mandates that trades and businesses "aggregate related transactions" in order to prevent money launderers from spreading out an order over time to avoid filing requirements.[33] Consequently, willful failure to inform the IRS of such activity can result in criminal and civil penalties.[34]

At the same time, the United States's general legal approach to this issue is shaped by its membership in the twenty-six-nation Financial Action Task Force on Money Laundering ("FATF"), whose purpose is the development and promotion of policies to combat money laundering. In particular, as part of this organization, the United States has agreed to adopt and implement the forty FATF recommendations, issued in 1990 and revised in 1996, which set out the basic framework for anti-money laundering efforts worldwide. These recommendations "cover the criminal justice system and law enforcement; the financial system and its regulation; and international cooperation."[35] Similar to many of the

---

30. *See id.* at 682-83.

31. Section 1956 adopted a very broad approach in defining the types of financial transactions falling within the scope of the MLCA, including almost all forms of commercial activity. *See* 18 U.S.C. § 1956(c)(4) (1994). The only requirement is that the transaction must either affect "interstate or foreign commerce" or be conducted through or by a financial institution that is engaged in activities affecting that commerce in any way. *Id.* Section 1957 makes it a crime to engage in monetary transactions in property derived from specified unlawful activity. *See* 18 U.S.C. § 1957 (1994). As is true under section 1956, a key component in the criminal violation is a knowing receipt of criminally derived funds over $10,000 when it involves a financial institution at some stage during the transaction. *See id.*

32. 26 U.S.C. § 6050I (1994).

33. *Id.*

34. *See id.* Also included in the legal framework, but not particularly relevant for our purposes here, is forfeiture (18 U.S.C. §§ 981–982), which provides that any property "involved in a transaction or attempted transaction in violation of [money laundering statutes] or any property traceable to such property" is forfeitable to the United States. "Property involved" includes any property used to facilitate the laundering offense. *See* 18 U.S.C. § 981 (1994).

35. FINANCIAL ACTION TASK FORCE, FINANCIAL ACTION TASK FORCE PAPER ON MONEY LAUNDERING (1996) [hereinafter FATF PAPER] *available at* <http://www.usis-israel.org.il/publish/econews/1996/ecojuly/eco701b.htm> at introduction para. 4. The recommendations are not intended to serve as a prescription for every country's efforts

concepts set out in U.S. legislation, the forty recommendations strongly encourage financial institutions to keep ordered records of customers and verify the legal structure of any business customers.[36] Many of the principles go even further than some American legislation, however, and in so doing provide useful guidelines for future enforcement efforts in this country.[37]

II. E-MONEY AND THE CHANGING DYNAMIC OF MONEY LAUNDERING

A. The Basic Structure of E-Money Systems

In order to fully evaluate the unique threats that electronic money poses to anti-money laundering efforts in the United States, it is first necessary to have a basic understanding of the underlying technologies involved. On a general level, the term electronic money ("e-money" or "e-cash") refers to a variety of mechanisms that will facilitate payments at stores and on the Internet through computer-based communication technologies.[38] These systems might involve the use of stored value cards ("SVCs") or "smart cards" to transfer funds in person or over the Internet; these systems might also utilize value stored on the hard drives of personal computers ("PCs"), transmitting some of that value to other PCs.

Many experts agree that, due to the rapid rate of development and change currently occurring in these technologies, an efficient way to distinguish among the emerging systems is to focus on the issuing entity

---

to combat money laundering. Rather, they are written with an understanding that the FATF countries have diverse legal and financial systems and cannot all take identical measures. "The Recommendations are therefore the principles for action in this field, *for countries to implement according to their particular circumstances and constitutional* frameworks . . . ." *Id.* at introduction para. 5.

36. *See* FATF REPORT, *supra* note 4, annex at para. 22.

37. For example, recommendation 12 offers a somewhat more pointed version of the "know your customer" principle, recommending that financial institutions maintain all necessary records on transactions, as well as on customer identification, for at least five years. *See* FATF PAPER, *supra* note 35, Forty Recommendations of the Task Force at para. 12.

38. *See* Catherine Lee Wilson, *Banking on the Net: Extending Bank Regulation to Electronic Money and Beyond*, 30 CREIGHTON L. REV. 671, 683–84 (1997). It is important to note that, currently, there is no formally adopted international terminology with respect to electronic money systems. Consequently, it may often be the case that the same terms, when mentioned in scholarly articles or cases, may have a slightly different meanings depending upon the specific context and circumstance.

and "whether the systems operate in an open or closed environment."[39] Accordingly, in its 1997 report, the FATF categorized e-money systems in four models: (1) the *merchant issuer model*, in which the card issuer and seller of goods and services are the same; (2) the *bank issuer model* for closed and open systems, in which the merchant and the card issuer are different parties, while transactions are cleared through traditional banking mechanisms; (3) the *non-bank issuer model*, where users buy e-money from issuers using real money, spend the e-money at participating merchants, and the issuers subsequently redeem the cash from the merchant; and (4) the *peer-to-peer model*, in which the bank or non-bank issues e-money, which is then transferable between users, with no interference by a financial institution except at the initial point of issuance and then at the redemption, if ever, of the e-money by individuals or merchants.[40] Among the various companies currently seeking to develop e-money systems, those most representative of the dominant trends in the industry, and also those nearest to full scale implementation in the United States, are DigiCash, CyberCash, Mondex, and Visa.

Developed by the Netherlands company DigiCash,[41] e-cash is an example of a *bank issuer model* e-money system that utilizes PCs to store value that can then be transmitted by buyers from remote locations to carry out various transactions. First, the user purchases digital "coins," unique serial numbers associated with a specific amount or denomination of monetary value, from their own bank.[42] Next, when the user requests e-cash value for a later transaction, the bank debits the user's account in the amount requested and the user's computer subsequently generates and stores the value as a set of random serial numbers in the value and denominations desired.[43] Then, when the user wants to make a purchase over the network, the user simply commands its computer to transfer the coins to the merchant's web page or bank account.[44] Finally, the merchant "validates" the coins, completing the exchange.[45]

---

39. *See* FATF REPORT, *supra* note 4, annex at para. 15.

40. *See id.*

41. *See* DigiCash, Welcome to Digicash (visited April 15, 1998) <http://www.digicash.com>.

42. Task Force on Stored-Value Cards, *A Commercial Lawyer's Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated with Stored-Value Cards and Electronic Money*, 52 BUS. LAW. 653, 660 (1997).

43. *See id.*

44. *See id.* at 660–61.

45. Coin "validation" in the e-cash system is able to be carried out by a merchant in one of two ways. Typically, at the time the "coins" are exchanged, the merchant's

Similarly, CyberCash, developed by CyberCash, Inc., is another computer-based stored value product, but one that operates on the non-bank issuer model. Under this system, a user can load coins either from a bank account or a credit card onto a CyberCash "wallet" stored on a user's computer. When a user loads the wallet, funds are transferred from the user's bank account to an account in a federally insured bank maintained by CyberCash. CyberCash accounts for all of the user's funds in his/her wallet.[46] Then, when the CyberCash holder finds something he wants to buy over the computer network, he only needs to click on the item on the screen to complete the transaction. With the click of the mouse, an almost instantaneous process occurs: the user's electronic wallet on the computer is activated; coins are collected from the wallet to update the user's balance; the coins are delivered by CyberCash to the merchant as payment; and the product is sent to the user, either electronically over the Internet (e.g., news services) or through the mail.[47] Finally, all transaction information is passed through a central database maintained by CyberCash, but the files are not accessible to CyberCash unless the user unloads the files with the user's own private key.[48]

In contrast to CyberCash's and DigiCash's computer based systems, the Mondex[49] model of stored value systems involves the use of pre-programmed smart cards that can be repeatedly loaded with value to pay

---

software automatically sends the "coin" to the issuer for validation. Before completing the transaction, the merchant can choose to either wait for the issuer's assurance that the coin has not been previously spent (considered online verification) or can instead use the bank's "public key" to merely authenticate the coin's existence on its own (considered offline verification). *See* Task Force on Stored-Value Cards, *supra* note 42, at 661. This method will not assure the merchant that the coin has not been spent, but this choice does cut down on the time and hassle of the transaction for both parties. Moreover, to ensure the privacy of the user, e-cash coins are designed so that, even if their authenticity is verified online, neither the identity nor the location of the payor, requester of the authentication, or the hard drive on which the coin is stored, is ever revealed to the bank. *See id.*

46. *Id.* at 661. It is important to note that this is a sharp contrast from e-cash, which maintains no such central holding institution for funds separate from the user's regular bank.

47. *See id.* at 662.

48. *See id.* This too is considered online verification. "All of the information transmitted on the Internet between a user and CyberCash is encrypted. The transactions are processed using security systems designed to preserve data security. An encrypted archival copy of all transactions is maintained on CyberCash servers." *Id.*

49. Mondex was formed as a joint venture of Chase Manhattan Bank, AT&T, Wells Fargo Bank, along with four other big banks and credit-card companies. Mondex can be researched at its website, <http://www.mondex.com>.

for items either online or in person, namely by swiping the cards through special readers at the point of sale.[50] In general, the Mondex model is a hybrid of the *non-bank issuer* and *peer-to-peer models* as designated by the FATF. Based on a multi-step distribution process, the model starts with an entity called the "originator," which issues and redeems Mondex value in the local currency to distributing member institutions ("members"). These members, in turn, will "pay the originator for the issued 'value' and the originator will earn investment income and float on the amount paid by the member during the time period between receipt of payment and future settlement of the value."[51] Members, then, sell the Mondex value to, and collect it from, users.

Mondex value can both be stored on a smart card and used in several different ways. For example, value can be loaded and reloaded from an automatic teller machine ("ATM"), over the telephone or personal computer, or through a special floppy-based device called a "wallet."[52] Regarding the use of Mondex value, the smart card allows holders to make purchases over the web; download cash from a bank, an ATM, or a network; and pay for merchandise in stores or vending machines. In sharp contrast to e-cash and CyberCash, however, the Mondex system also enables users to make card-to-card transfers using electronic wallets without any interaction or knowledge of a third party (e.g., bank, merchant). This is due to the fact that there is no centralized system for transactions in the Mondex model. Rather, as transactions occur, value is subtracted from one card and added to another to be used in other transactions. While the holder of that value can transmit the relevant information to the issuer of the card and get payment, the expectation is that the electronic value will simply circulate among individuals and entities participating in the system.[53]

---

50. *See* Kim Nash, *Cybercash at Risk: Money Laws Lacking*, COMPUTERWORLD, Dec. 23, 1996/Jan. 2, 1997, at 1, 16. To the average observer, smart cards look very similar in appearance to conventional credit cards. In fact, the only really noticeable difference between them is the presence of a microchip, embedded in the smart card and visible to the user, rather than a magnetic strip on the back of regular credit cards.

51. Task Force on Stored-Value Cards, *supra* note 42, at 660.

52. *See* Christy Hudgins-Bonafield, *Can Smartcards Unlock Electronic Cash Vaults*, NETWORK COMPUTING, July 1, 1997, at 24. Wallets also enable the card user to keep track of the balance on the card, as well as a record of the last ten transactions.

53. *See* John L. Douglas, *The FDIC, Taking a Different Approach from the Federal Reserve, Weighs in on How Regulations of Deposits Apply to Stored Value Cards*, NAT'L L.J., Aug. 26, 1996, at B4. As an example of how this system works, imagine that a mother wanted to give her son $10 for his weekly allowance. Assuming that both mother and son have Mondex cards, the mother would first slip her own card into her electronic wallet and transfer $10 in electronic value onto the wallet's computer chip.

Somewhat similar in function to the Mondex system is VisaCash, introduced at the Atlanta Olympics by Visa, which uses disposable or reloadable SVCs enabling holders to carry out low dollar value consumer transactions. By contrast, however, the Visa value that is collected by merchants is cleared between participating banks using Visa's existing clearing system and through the settlement arrangements currently in use for Visa credit card transactions.[54] Consequently, unmonitored and unregulated peer-to-peer transfers are not allowed. Moreover, with VisaCash, all transactions are offline in that there is no centralized offline verification of the card holder or the transaction.[55]

The magnitude of the benefits that these e-money products offer to consumers remains unclear due to their current lack of widespread adoption.[56] In general, however, industry analysts agree that e-money systems, at their most basic level, stand ready to present users with all of the advantages of traditional currencies and much more. For example, all e-money products developed now and in the future will most likely offer consumers a "store of value, a medium of exchange, a numeraire . . . and convenience," just like traditional currencies and paper monies.[57] Similarly, they create the potential for complete anonymity of the user, as wire transfers currently do to a certain extent. They also allow currency to be transferred almost instantaneously from point to point, and for bulky paper currencies to be replaced with intangible, easily manipulable electrons.[58]

Then, she would slip her son's empty card into the wallet and transfer the value onto that card. At that point, the son could use the card for purchases at various stores that are equipped to handle the Mondex cards. Similarly, a customer could walk into a hardware store and purchase supplies with his Mondex card for $100. The necessary value would be subtracted from the user's card balance at the end of the transaction, and transferred to the merchant's wallet or computer system. Then, instead of redeeming the value for currency, the merchant might instead use the same value to pay his bills and transfer the original value to those suppliers who also used the Mondex system. In this regard, according to one scholar, Mondex value is "probably the closest electronic equivalent to actual cash." Hudgins-Bonafield, *supra* note52, at 25.

54. *See* Task Force of Stored-Value Cards, *supra* note 42, at 660.

55. *See* Douglas, *supra* note53, at B4.

56. *See* GROUP OF TEN, *supra* note 19, at 6.

57. *Money Laundering Via Smart Cards*, REPORT ON SMART CARDS, Mar. 17, 1997, at 4, *available in* 1997 WL 8987475.

58. *Id.*

In a recent study, the Group of Ten[59] suggested that e-money systems might also provide users with the additional benefits of a less expensive payment method, a faster and more convenient means of payment, and an increase in the variety of payment options.[60] Similarly, e-money might also present fewer risks for consumers than many extant forms of payment.[61] The prepaid nature of e-money could result in a lower risk of refusal than in traditional exchanges, such as when a credit card is expired or deactivated or when a merchant is unable to make change for currency or refuses to accept a personal check. This feature might reduce the risk that a consumer would be unable to complete a payment in the amount or at the time and location they desire despite having enough money in an account to cover the transaction.[62]

B. The Dangers E-Money Presents to Conventional Money Laundering Enforcement

Despite the readily apparent benefits of e-money products, most industry and law enforcement analysts agree that the current schemes for e-money pose potentially devastating threats to traditional anti-money laundering efforts. In general, certain elements inherent in the premise of e-money systems, as currently developed, would make conventional means of tracking funds and conducting surveillance of laundering activities virtually meaningless. Consequently, e-money systems could provide money launderers with a new way of transferring their illegal funds all over the world, in an instant, and in a way that would be virtually undetectable by law enforcement. These effects could be quite significant.

While the list of potential threats to anti-money laundering efforts is conceivably endless due to the unfinished nature of most e-money systems, it is still necessary to grapple with some of the more pressing and already identifiable threats. For example, one of the most potentially problematic features of e-money systems is the ability to transfer value between individuals rather than just to or from merchants, because this feature affects the degree to which criminals can use e-money effectively by limiting the amount of information that can be

---

59. The Group of Ten Working Party on Electronic Money is comprised of representatives from finance ministries, central banks, and international organizations brought together under the auspices of the Group of Seven Heads of State and Government.

60. *See* GROUP OF TEN, *supra* note 19, at 6.

61. *See id.* at 7.

62. *See id.*

collected by a central entity (e.g., a bank). Consequently, this feature would reduce the effectiveness of traditional transaction monitoring,[63] since the central operator would not be able to check security parameters on the card in order to look for laundering activity.[64]

This greater transferability would most likely provide criminals with an attractive new tool for maintaining their ongoing businesses by allowing them to make large payments directly and anonymously to individuals or corporations in other jurisdictions.[65] Using the Mondex model as an example, a criminal could load $50,000 from his fake corporate account onto a smart card and transfer the value any number of times between different corporations controlled by his organization. While the initial withdrawal would be recorded and eventually reported by the financial institution holding the original account, any transfer after that point could occur without any supervision or paper trail. Ultimately, by the time the criminal's last shell company cashed in its card's value with a member bank, there would be no way of tracing the origin or destination of the money. Along the same lines, it is easy to imagine some Internet-based e-money systems being utilized to launder funds without any detection or identification of the participants.[66]

Closely connected to the idea of interpersonal transferability is the issue of whether there will remain any intermediaries in these new payment schemes and what the effects would be if they were taken away. Under the current regulatory regime, the financial institutions listed in section 5312 of the BSA (e.g., banks, securities brokers, check cashiers) are able to serve as the stopgaps for conventional laundering

---

63. *See* COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS & GROUP OF COMPUTER EXPERTS OF THE CENTRAL BANKS OF THE GROUP OF TEN COUNTRIES, SECURITY OF ELECTRONIC MONEY 18 (1996) [hereinafter COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS].

64. *See id.* at 19.

65. *See* GROUP OF TEN, *supra* note 19, at 25–26.

66. A possible scenario involving money laundering over the Internet would be where one front corporation orders a piece of industrial machinery offered for sale on the Internet by a conspiring company. The e-money user would go to the company's web page and click on the item of machinery it wanted, subsequently downloading the appropriate value (for example, $9,000) from his PC. No machinery is ever sent, though, since this is in reality a false transaction. Then, after sending out a phony invoice to the original purchaser for the machine, the second company could transfer the value now on his computer to a front production corporation, where a false receivable account has been previously set up to mark the initial sale of the machinery to the distributor. At this point, there has been no online verification of the funds or any monitoring of the transaction by any regulatory authority. Eventually, when the production company sends the value to be redeemed by a financial institution for cash, the money has been completely laundered.

mechanisms (e.g., wire transfers, checks).[67] More specifically, information regarding the dollar amounts and the frequency of transactions can be collected there and made available to enforcement agencies for examination. By contrast, offline systems do not require banks as funnels for cash and can avoid them altogether. Until one of the recipients deposits the cash, the bank only knows the identity of the individual who originally withdrew the "coins." It is very unlikely that money launderers would ever cooperate with law enforcement by giving them the identity of each consecutive spender of the coin. As a result, it would become impossible to track any of the later transactions involving the initial withdrawal.[68]

Another threat inherent in the design of e-money products involves their current technological capacity to hold unlimited amounts of value. If SVCs or the hard drive of a PC could hold thousands or even millions of dollars of value, they could make it significantly easier for criminals to transfer large, anonymous payments to individuals in any number of jurisdictions around the world. For example, a criminal could carry a SVC in his pocket with a million dollars of value onto a plane to another country. The SVC would look just like any other credit card, and authorities would have no more reason to search the courier at the airport than they currently do to search any other passenger. This possibility would substantially eliminate the need and the utility of smuggling the same funds out of the United States through much riskier methods. Even if there were a value limit placed on consumer-owned SVCs, like some current products, criminals still would be able to take advantage of the higher value limits available to merchants to accommodate the volume of retail transactions. In truth, money launderers could use the merchants as fronts, storing large amounts of funds on the merchant terminals with much less suspicion from regulators.

Finally, the emerging e-money systems may also make it increasingly difficult for vendors to know their customers, to keep certain transactional records, as well as to authenticate the legal structure of business customers.[69] Similarly, verifying the true identity of persons conducting transactions over a period of several years would also be difficult with some of the new systems.[70] The variances in record-

---

67. *See* 31 U.S.C. § 5312 (1994); *see also supra* Part I (discussing how this mechanism works under the Bank Secrecy Act).

68. *See* Laurie Law, *How to Make a Mint: The Cryptography of Anonymous Electronic Cash*, 46 AM. U. L. REV. 1131, 1150 (1997).

69. *See* FATF PAPER, *supra* note 35, at "Forty Recommendations," paras. 10–12 (recommending financial system actions to combat money launderers).

70. *See generally id.* para. 12.

keeping among the different e-money systems places traditional law enforcement tools in jeopardy. In particular, while some e-money schemes would verify every transaction that was executed, most others, if allowed, would likely exercise the less expensive option of checking on an ad hoc basis or in response to suspicious behavior.[71] Some issuers have even suggested that they anticipate offering SVCs through vending machines, in which case the transactions of a particular card might be tracked but not the identity of the user.[72] Generally speaking, the fewer records maintained by a financial institution, especially when opening the account, the better for criminals engaged in money laundering.

Similarly, the potential for rapid movement of incredibly large numbers of e-money transactions over the Internet may also make it difficult for law enforcement to identify or track transfers of illegal funds. The FATF described this threat in 1997, stating:

> Once e-money systems are used on a large scale, they will also handle a certain amount of these illicit funds. While it is not anticipated that e-money will consist of the same value as the wire system, it may consist of a larger volume of transactions, thus illegal funds may be even more difficult to find if only because of the sheer volume of funds circulating within the system. The mass volume and the speed of processing of computerized data will make it difficult to develop indicators to detect suspicious activity.[73]

At the same time, this feature of e-money systems would also make it financially impractical for financial institutions to record the aggregate cash flows of their transactions or to implement currency reporting regimes.[74] Both of these recording methods are useful safeguards against money laundering.

Evaluating these potential threats, experts in law enforcement and cyber-crime have predicted dire consequences for the future of anti-money laundering efforts and society. For example, Michael Nelson, a Clinton Administration official on information security and cryptography matters, foresees, that "traditional notions of sovereignty, national security and warfare will be undermined by the year 2020, when

---

71. *See* COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS, *supra* note 63, at 18.
72. *See* GROUP OF TEN, *supra* note 19, at 15.
73. FATF REPORT, *supra* note 4, at 22–23.
74. *See id.* annex at para. 38.

the whole world is wired and e-cash is the norm."[75] Others predict that money laundering will be completely undetectable and unpreventable, and consequently governments will become less powerful in relation to criminal organizations.[76]

III. E-MONEY SYSTEMS: THE FEDERAL GOVERNMENT'S CURRENT APPROACH AND ITS PROBLEMS

Despite the apparent significance of the threats posed by emerging e-money systems, the U.S. government's current approach is surprisingly inadequate and shortsighted, and fails to address the problems associated with money laundering. The result is an environment that is not beneficial for the emerging e-money industry, the American consumer, or the United States as a whole.

A. The Government's Current Approach

In general, the U.S. government has consistently refused to take a definitive stand on how e-money should be treated under American laws, most significantly, anti-money laundering laws. The government has yet to decide some of the most basic issues surrounding e-money. For example, is the value stored on e-money products a form of legal tender or some other form of currency and thus subject to the existing framework regulating financial transfers?[77] The federal government has chosen to follow a "wait and see" approach regarding e-money and money laundering. This inaction can be attributed to the federal government's general view that it is too early for the creation of regulations and to the widespread opinion that the technologies underlying SVCs and Internet payment systems are "still in [their]

---

75. Richard L. Field, *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, 1020 (1997).

76. *See* Graeme Browning, *Cybercops and Robbers*, NAT'L J., Mar. 22, 1997, at 1.

77. According to Catherine Lee Wilson, "[t]he ability to serve as 'legal tender' defines money in the commercial law context." Wilson, *supra* note 38, at 691. Of equal importance in this context is the fact that the UCC defines "money" as "a medium of exchange authorized or adopted by a domestic or foreign government and includes a monetary unit of account established by a governmental organization or by agreement between two or more nations." U.C.C. § 1-201(24) (1995). Because the federal government has not yet adopted SVCs specifically, or e-money generally, as a medium of exchange, "the value placed on stored value cards and personal computers will not constitute money for commercial law purposes." Wilson, *supra* note 38, at 691.

infancy."[78] Many experts and government officials, consequently, have concluded that e-money products should be allowed to develop in a competitive marketplace free of legal restrictions before any systematic attempt is made to regulate them.[79]

Defending their position, government officials and industry experts have argued that it is not only uncertain whether e-money systems will ever receive widespread acceptance in the United States, but also whether they will ever appeal to potential money launderers. Indeed, with the exception of isolated bank experiments in a few U.S. cities,[80] most e-money products have yet to receive widespread distribution or use within the United States. Perhaps because most of the products have been designed for, or used in, low-value consumer and retail transactions (typically considered to be unattractive to money laundering schemes),[81] no evidence of money laundering has yet been detected or suspected involving the products used within the United States.[82] Government officials thus believe that they are justified in acting as if it is "premature to consider prescriptive solutions to theoretical problems."[83]

In order to get a firmer handle on the multitude of issues and dangers that this technology could present, the United States has chosen to study these new technologies exhaustively. As an illustration, in 1995, Alan Blinder, former vice-chairman of the Federal Reserve Board, accurately reflected the U.S. government's position, then and now, when he said, "the uncertainties regarding the future of 'e-money' are so overwhelming that we mainly suggest patience and study rather than regulatory restrictions."[84] Simultaneously, law enforcement officials and regulators have made efforts to cooperate with the e-money industry in order to understand emerging issues and to share with them potential law

---

78. Report on Smart Cards, *supra* note 57, at 4 (quoting Stanley Morris, director of FinCEN, commenting on the FATF meeting of July 1, 1996).

79. *See* Mark E. Budnitz, *Stored Value Cards and the Consumer: The Need for Regulation*, 46 AM. U. L. REV. 1027, 1029 (1997).

80. Four cities have bank experiments in e-money systems: Kansas City, Missouri; St. Louis; New York City; and Atlanta.

81. *See* Budnitz, *supra* note79.

82. *Security: Money Laundering and the Net*, AM. BANKER, May 12, 1997, at 1. Several industry experts have also spoken out in support of the government's view. For example, Richard Insley, vice president of Signet Bank, recently said he thought it was unlikely that money launderers would convert dollars to digital cash and then shop around the Web for small-dollar items that could be reconverted back to cash at a discount. *See id.* Similarly, Anne Friedman, vice president of Chase-Manhattan Bank, opined that "criminals like inefficiency . . . . And these (e-cash systems) are very efficient systems." *Id.*

83. FATF PAPER, *supra* note 35, at 15.

84. *Internet Crime, What a Tangled Web*, EUROMONEY MAG., Oct. 15, 1996, at 84.

enforcement concerns generated by their products.[85] As of yet, however, no official suggestions or proposals from any of these groups have been universally adopted and applied by the federal government. Consequently, the laws that govern digital money remain unclear.

B. The Problems with this Approach

In light of all the evidence, the government's "wait and see" approach is not the most appropriate or beneficial one for consumers, law enforcement, or society as a whole. For example, for those involved in the electronic commerce and finance industries, the widespread utilization of e-money products in the United States is imminent, perhaps arriving within the next three to seven years.[86] E-money developers will likely continue their efforts to make these technologies widely available to consumers who want them.[87] It is also reasonable to conclude that the consumer demand for these products will strenghten once they actually arrive. Based on results from test cases conducted in Europe, Asia, and certain cities within the United States, e-money companies are optimistic that American consumers will choose to adopt this new technology as a replacement form of currency in many types of transactions.[88]

---

85. *See* GROUP OF TEN, *supra* note 19, at 18; FATF PAPER, *supra* note 35, at 15. For example, the FATF; FinCEN; the Federal Reserve Board, *see* Field, *supra* note 75, at 981; and the President's Commission on Critical Infrastructure Protection, *see id.* at 1019–20, to name a few, have all recently enlisted the help of e-money industry experts in order to identify and crystallize potential issues and new challenges to law enforcement.

86. *See* Hudgins-Bonafield, *supra* note 52, at 2.

87. According to Gregory Maggs, these efforts to create and implement new payment devices almost certainly will continue for two reasons. First, current technological advances are making new payment devices easier to create and implement. Specifically, computers and improved communication networks are now able to solve many old problems that may have discouraged similar enterprises from proceeding with similarly risky currency ventures in the past. Second, the potentially massive revenues that new payment devices could generate for their developers provide a very strong incentive to develop these technologies in order to compete with existing devices and to capture market share. *See* Gregory E. Maggs, *New Payment Devices and General Principles of Payment Law*, 72 NOTRE DAME L. REV. 753, 765 (1997). For example, Input, Inc., a California based consulting firm, expects electronic payments on the Net to surge from $60 billion in 1994 to more than $250 billion in 1999. *See* Browning, *supra* note 76, at 1; *see also Security: Money Laundering and the Net*, *supra* note 82, at 1 ("New York-based research firm Jupiter Communications predicts that on-line commerce will be a $7.3 billion market by 2000; about half of that business will be transacted using smart cards, e-cash, and e-checks.").

88. For example, Mondex found in a recent English pilot program that 66% of the 10,000 total smart card holders preferred to use their Mondex card over cash. *See*

With the advent of these products potentially around the corner, the threats that e-money systems pose in theory could soon become a reality. Indeed, the dangers are especially great in a marketplace that is currently unregulated by the federal government. Manufacturers have a strong incentive to provide consumers with the least expensive and most flexible product. In such a relatively young, untested industry, manufacturers would dispense with important anti-money laundering features if they were expensive to produce or limited the devices' applications. For example, most e-money providers might choose, if allowed, to provide only ad hoc verifications of transactions, despite the enhanced ability of money launderers to hide their identities, because ad hoc verifications cost significantly less than verifications of all transactions. Unregulated, therefore, e-money providers may jeopardize the very safety nets that government regulators have created with conventional anti-money laundering provisions.

Ironically, it is also possible that the lack of federal regulation of e-money actually hurts the industry, negating the government's aim of allowing it to flourish unfettered by limitations. According to one scholar, "[a] barrier to widespread electronic commerce is the absence of a legal infrastructure at the application level."[89] This legal uncertainty has made it difficult "for developers and users to ascertain, control, and appropriately limit risk."[90] The currently limited scope of government regulation has created the possibility that companies, which today are free to design their systems as they choose, may be forced to take expensive corrective action in the future as the dangers to law enforcement are realized. For example, a company that previously operated on a peer-to-peer model, e.g., Mondex, could eventually be forced to develop a central clearing agency just to stay in business.

Finally, given the potential for criminal behavior in the current environment, it seems worthwhile to consider whether any alternative approaches exist that might reduce these risks. Indeed, the following section suggests that the United States does, in fact, have other options; they currently have enough information, knowledge, and understanding

---

Wilson, *supra* note 38, at 682. Add to this the existence of a pre-established base of potential users of e-money, including a portion of the 30 million worldwide users of the Internet, the 35 million U.S. households with personal computers, and "over 98 million households if a more advanced type of telephone or interactive television technology takes hold in the United States," *id.* at 673, and, ideally, e-money could soon replace a substantial portion of the approximately $400 billion of U.S. currency circulating worldwide. *See id.*

89. Field, *supra* note 75, at 984.

90. *See* Task Force on Stored-Value Cards, *supra* note 42, at 655.

of e-money and money laundering to establish regulations aimed at preventing criminal activity. A proposed framework is also described in this section.

IV. An Alternative Approach to E-Money

This section offers an alternative approach to the issue of e-money regulation as it relates to use in money laundering. Drawing from the government's experiences in other areas of commercial law, its experiences with money laundering, as well as its recent studies of e-money, a three part strategy is considered. First, the U.S. government should take decisive regulatory action in order to shape the future development of the industry. Second, it should lay the foundation for the establishment of a dynamic framework for e-money systems. Finally, in order to eliminate the attractiveness of e-money systems to money launderers, the government should flesh out this basic framework with several proposals that dictate what specific designs are permitted.

A. Shape the Future Development of the Industry Through Regulation Now

To avoid the problems with e-money as they relate to money laundering, the government should take decisive steps now to regulate the emerging industry of e-money. This aggressive posture could result in less overall risk of financial loss for the companies themselves. It could significantly reduce the chances that criminals would be able to take immediate advantage of e-money products for money laundering when they became available. Fortunately, due to its early and extensive consideration of the regulatory issues, the government is presently capable of formulating a coherent and comprehensive scheme of regulation.[91]

A map for future action can be found, at least in part, in the government's successful treatment of digital audio tape systems as they relate to U.S. copyright law. In October 1992, for the first time in this area of the law, Congress enacted legislation specifically addressing the problem of private copying raised by the introduction of the digital audio tape ("DAT").[92] As a new form of private copying medium, DATs possess superior recording capabilities and permit an apparently infinite number of generations of copies to be made without loss of sound

91. *See* Wilson, *supra* note 38, at 675.

92. *See* The Audio Home Recording Act of 1992, 17 U.S.C. §§ 1001–1010 (1994).

quality from copy to copy.[93] Consequently, songwriters and sound-recording producers feared that "private copies would substantially displace sales of authorized recordings."[94]

Rather than waiting to see if these fears were realized, Congress chose to formulate legislation that not only adapted copyright law, but also imposed a "technological fix."[95] Specifically, by working in cooperation with industry representatives, Congress was able to establish a provision that obliges manufacturers and importers to include a device[96] that disables the machines' ability to record a copy from a prior copy in all consumer digital audio tape machines. In the end, the government helped shape the direction of the industry in a way such that the interests and concerns of both law enforcement and the DAT industry were met. And while this experience stems from copyright law, there is little reason to think that the same framework could not be utilized effectively to prevent e-money from becoming the unchecked tool of money launderers.

B. Laying the Basic Foundations for a Dynamic Framework

Since the U.S. government is heavily involved in international and national organizations studying the dangers of money laundering and e-money, it should officially recognize that e-cash constitutes a fundamentally new class of electronic payment instruments. In the last five years no fewer than six different government organizations studying this issue have made such pronouncements.[97] Consequently, the government should either revise the old laws or create a new set of regulations specifically targeted toward the unique threats presented by e-money.

In order to ensure that any attempts to shape the development of products will affect the entire e-money industry equally, any set of laws should treat all issuers of e-money as financial institutions subject to the applicable regulatory framework. Experiences and discussions with the technology industry also make it clear that any new rules in this area

---

93. *See* ROBERT A. GORMAN & JANE C. GINSBURG, COPYRIGHT FOR THE NINETIES 459 (1993).

94. *Id.* at 459.

95. *Id.*

96. The device is called a serial copy management system ("SCMS"). *See id.* at 460.

97. This group includes the FATF, Group of Ten, FinCEN, the President's Executive Committee, Alan Blinder of the Federal Reserve Board and the Office of the Comptroller of the Currency.

need to account for the rapidly changing nature of the technology. These laws should also serve as a jumping off point for the more detailed regulations necessary to address new threats to anti-money laundering efforts. To that end, the creators of the new regulatory framework would benefit from focusing their attention on the essential design features of e-money systems, which are less prone to radical change, rather than on the actual technical implementation of the products themselves.[98] Along the same lines, the lawmakers should pay special attention to the scope of their definitions of e-money systems so that they are neither too broad nor too narrow.[99]

The importance of such a dynamic regulatory framework can be seen from a brief look at the federal government's rather recent, and arguably unsuccessful attempt at the regulation of "swaps."[100] As discussed in a recent article by Professor Henry Hu, the financial device of swaps represents a revolutionary way of hedging and managing risk for investors. In the most basic sense, a swap is a type of derivative. Professor Hu concludes that the regulatory framework set up to manage the new risks presented by swaps[101] has failed to achieve its intended purpose. This, he suggests convincingly, is largely the result of indifference on the part of lawmakers "to the underlying process of financial innovation by which financial products continue to arise and evolve."[102] Swaps can be considered rather similar to e-money systems, which also redefine the traditional parameters of financial transactions. As such, regulators need to "analyze systematically the full range of possible changes . . . which would render the internal regulatory system more accommodating of the financial innovation process."[103]

Finally, the government should include the formation of a large, federal supervisory agency to collect, analyze and monitor e-money transaction information. E-money intermediaries would send data to this

---

98. *See* Simon L. Lelieveldt, *How to Regulate Electronic Cash: An Overview of Regulatory Issues and Strategies*, 46 AM. U. L. REV. 1163, 1165 (1997).

99. *See* FATF PAPER, *supra* note 35, at 20.

100. For a more in-depth discussion on the different types of swaps being used in the financial markets today, see Henry Hu, *Swaps, The Modern Process of Financial Innovation and the Vulnerability of a Regulatory Paradigm*, 138 U. PA. L. REV. 333 (1989). It should be noted that the specific elements and functions of "swaps" are not particularly relevant here. Swaps merely represent another product of financial innovation that create new risks not directly addressed by the pre-existing regulatory framework.

101. The framework established is entitled the International Convergence of Capital Measurement and Capital Standards (the "BIS accord").

102. Hu, *supra* note 100, at 335.

103. *Id.*

agency for the purpose of detecting money laundering activities. Building upon the FATF's Forty Recommendations,[104] this organization should be a distinct entity, separate from the Treasury Department, and its structure should be based on the centralized information units, Financial Intelligence Units ("FIU") currently used in several FATF countries. It would be responsible for monitoring the e-money industry and its issuers' compliance with the applicable federal regulations. As part of that role, it would be in charge of assigning the appropriate penalty, based on the pre-established guidelines in the MLCA for financial institutions,[105] for companies that failed to meet the requirements of the regulations.

The President's Commission on Organized Crime provided support for this idea when it pointed out the debilitating effect of an understaffed, overburdened supervisory agency on anti-laundering enforcement efforts.[106] The report noted that, because the relevant statute places the Treasury Department alone in charge of monitoring and investigating all cases of money laundering activity, other interested agencies have been unable to share these responsibilities for lack of jurisdiction.[107] As a result, it generally takes six to eight weeks for CTR data to be processed and made ready for analysis by the Treasury Department. That delay hampers the government's ability to move quickly and strategically against money laundering activities.

C. Proposals for Regulating the Design of E-Money Systems

The federal government, through Congress, should flesh out this basic framework with specific regulations establishing guidelines for the design of e-money systems. This set of regulations should draw upon and incorporate the lessons from past experiences with money laundering. Nevertheless, it is clear that most regulatory safeguards may be susceptible, at some point, to evasion. With that in mind, the

---

104. Recommendation 23 suggests that countries create a national central agency, which could store in a computerized data base all the reports of domestic and international currency transactions above a fixed amount sent to it by banks and other financial institutions. This information could then be made available to authorities for use in tracking and investigating potential money laundering cases, subject of course to strict safeguards to ensure proper use of the information. *See* FATF PAPER, *supra* note 35, para. 23.

105. *See* 18 U.S.C. § 981–982, 31 U.S.C. § 5324 (1994).

106. *See* PRESIDENT'S COMMISSION ON ORGANIZED CRIME, *supra* note 2, at 17–18, 23–25.

107. *See* 31 U.S.C. § 5319 (1994); PRESIDENT'S COMMISSION ON ORGANIZED CRIME, *supra* note 2, at 87–88.

proposal that follows attempts to fix most problems of the currently unregulated market of e-money.

Congress would be well-advised to require that e-money developers and issuers to incorporate some type of intermediary into the processing of transactions. This would mean that funds would have to pass through intermediaries whenever they were transferred, at which point records of the transaction could be obtained and stored for later inspection by law enforcement. Companies could be given the freedom to meet this requirement through the use of new technologies or through more traditional means (i.e., requiring online verification for all transactions). An intermediary is crucial since, "to the extent that greater transferability between users limits information collected by a central point, it reduces the effectiveness of transaction monitoring."[108]

The government should regulate an e-money developer's ability to provide untraceable currency products. Under this law, all e-money products would be required to provide some means for law enforcement or supervisory agencies to trace the source and destination of every transaction. Issuers would have to maintain a registry of the identity and address of the holders of their devices and give this information to a central authority. At the same time, legislative safeguards, such as requiring a warrant before giving access to the information, should be established to protect the privacy interests of consumers.

Experience has shown that anonymity poses an extreme threat to the detection of laundering activities. Indeed, one of the most valuable weapons in the fight against traditional laundering was the strong "know your customer" policy adopted by the financial institution conducting the transaction. This typically enabled financial institutions to trace both forward and backward[109] transactions, helping law enforcement officials catch money launderers by revealing who had paid, or who had been paid by, the suspected criminal. Without this type of safeguard, it might be impossible to link withdrawals with their deposits, which would prevent linking the payor and the payee in a criminal transaction.

Strict value limits, in the form of reporting requirements for funds transfers, have also proven to be a strong deterrent to laundering activities. In particular, the $10,000 barrier for the CTRs, CMIRs and FBARs significantly prohibits money launderers from simply transferring unlimited funds through financial institutions. Thus, the

---

108. COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS, *supra* note 63, at 18.

109. "Forward Traceability is the ability to identify a deposit record (and thus the payee) given a withdrawal record (and thus the identity of the payer). . . . [B]ackward traceability is the ability to identify a withdrawal record (and thus the payer) given a deposit record (and thus the identity of the payee)." Law, *supra* note 68, at 1159.

federal government would be wise to impose appropriate value limits on all card-based and software-based stored value systems, to be determined every few years by a joint committee of industry and law enforcement experts. The lower the amounts that can be transacted through any payment medium, the less attractive they are to the criminal element, which tends to deal in very large amounts of currency. Consequently, the appeal to money launderers of any e-money product could be substantially reduced if the value limits were kept relatively low and the system was designed primarily for low-end transactions.

Finally, all e-money issuers need to be included under the jurisdiction of the regulations in order to ensure access to the necessary information necessary for monitoring purposes. As the 1984 report of the President's Commission illustrated, it is very important to be able effectively to evaluate compliance effectively with whatever regulatory scheme the government establishes.[110] E-money providers should be required to work with the controlling supervisory agency, discussed above, to establish the most reasonable and productive time frame for the delivery of transactional records. Such a provision hopefully would cut down on the time lag between use and verification of e-money products, aiding in the early detection of laundering activities by law enforcement officials.

V. EVALUATING THE POSITIVES AND NEGATIVES OF SUCH A PROPOSAL

Of course it is not hard to imagine the existence of a large group of dissenters who feel that this proposed plan is unwise, inappropriate, and potentially harmful to the American economy, and many of those concerns would be well-founded. When these concerns are considered in light of all the available information and weighed against all of the positive aspects of the proposal, however, one should still be able to conclude that a more aggressive and pointed approach to e-money is the desireable approach.

A. Acknowledging and Addressing the Concerns of Dissenters

To begin with, certain features of the proposal might jeopardize the legitimate privacy interests of e-money users (i.e., consumers and merchants). Specifically, by requiring companies to stockpile detailed information on their users' identities, the federal regulations raise the

110. *See* PRESIDENT'S COMMISSION ON ORGANIZED CRIME, *supra* note 2, at 23–25.

possibility that this data could somehow find its way into the wrong hands and could be used against members unfairly. For example, law enforcement officials could conceivably, in an unregulated environment, attempt to break into an e-money company's database, or demand that information be handed over by a company, any time they suspected that an individual was involved in laundering funds using e-money. Provisions requiring law enforcement agents to follow the federal warrant procedures before obtaining this data would block government searches into users' personal information. Such requirements would provide some assurance that e-money users, criminals or not, would be afforded at least the same level of privacy protection as they would under conventional criminal laws.

In addition, many of the companies would not have access to this kind of personal information without the user's electronic authorization. The CyberCash system, for example, is designed so that a user's personal transaction records remain locked, unaccessible to a CyberCash employee, until the user "unloads" the files with his own private key. At the same time, however, not all e-money providers currently offer this type of protection and there is no guarantee that they will provide it in the future. With a product like Mondex, where the independent distributors (i.e., members) are allowed to keep track of transactions as they see fit, there is the possibility of a violation of a user's privacy. Overall, this issue requires further consideration as to whether additional regulatory safeguards should be established.

As another consideration, some e-money companies will be forced to endure the huge initial costs of altering their systems to meet the new regulations. All things considered, this is a likely event and one which provides grounds for caution, since the proposal's purpose is not to bankrupt these young companies. However, as discussed previously, by front-loading their costs and addressing the government's concerns now, companies might actually solidify their current financial positions by decreasing the risk of being saddled with large, unexpected costs later on. The expenses that e-money companies would incur by incorporating additional safety mechanisms into their products at the developmental stage would be much less than if they had to reshape their finished designs after they had already gone to market. Furthermore, because almost no e-money products are out in full scale yet, companies might also be able to reduce the overall cost of any design changes by deducting them as either start-up, or research and development expenses under corporate tax laws. At the same time, companies would not face the full brunt of these expenses alone, but rather they would be offset to a certain extent by the benefits paid for by the government. In particular, the proposed federal clearinghouse would take over some of the

monitoring and supervisory duties for which companies would typically have been solely responsible in an unregulated market.

And yet, other industry insiders could still complain that, because e-money products are still in their relatively early existence, any comprehensive regulation of the industry at this stage would stifle their development. In effect, they argue, regulations aimed at the products could unduly influence the direction of further development and, in the process, companies could be discouraged from bringing the most efficient and safe products to the market for fear of governmental retribution. According to Stanley Morris, this phenomenon is unfortunately all too common. He was recently quoted as saying "[t]oo often . . . government regulators have attempted to thwart a potential criminal threat by imposing burdensome regulations that reflect little appreciation of the nature of the threat, or the business practices of the affected industries. We cannot make the same mistakes with cyberpayment systems."[111]

If we accept the proposition that the federal government is capable of appreciating the needs of industry within a possible legal framework for e-money products, then federal regulation of e-money could actually provide significant benefits to the industry as a whole. By providing "a legal infrastructure at the application level,"[112] the federal government could limit the legal uncertainty that heretofore has made it difficult "for developers and users to ascertain, control and appropriately limit risk."[113] Considering that consumer confidence and trust is crucial to the future acceptance of e-money products, developers would certainly benefit from laws and regulations of e-money that would strengthen consumer protections by helping to maintain the universal integrity of electronic payment systems. The more confident a user of e-money can be that he is not part of the same system used by criminal organizations to launder money, the more willing he may be to continue using it.

Finally, the proposal does impose substantial new costs on the federal government. The largest source of these costs would be those necessary for the establishment, training and continued administration of the new central supervisory agency. These expenses would be in addition to those necessary to allow government officials to meet regularly with top industry officials to revise product standards, such as the lag time or value limits, as it becomes necessary to do so. Offsetting

---

111. *New Technologies Contain Potential for Massive Fraud*, BANKING POL. REP., Mar. 4–18, 1996, at 36.

112. Field, *supra* note 75, at 984.

113. Task Force of Stored-Value Cards, *supra* note 42, at 657.

some of these costs, however, would be the fact that e-money issuers would now have incentive to include the necessary security features in the products rather than face stiff penalties under the regulations. Consequently, these enhanced security measures might mean fewer monetary costs for the government, since some of their standard supervisory functions (i.e., identifying the parties involved in a transaction and gathering transactional records for analysis) would now be supplanted by e-money companies and their products. On a broader level, though, stricter security mechanisms could translate into the prevention of money laundering in the United States through these products. Because money laundering extracts such huge social costs, by providing criminal organizations and individuals with the means to finance their operations undetected, one could reasonably conclude that any costs necessary to produce this result might be outweighed by the enormous benefit they provide to the country as a whole.

B. Additional Strengths of the Proposal

There are some other benefits of the proposal that should be noted. As a general matter, many of them stem from the fact that the proposal takes advantage of certain features inherent in the federal government that enhance the likelihood of creating effective and efficient new regulations for e-money.

For one, the proposal places the most experienced and well-equipped organizations in charge of establishing and administering regulations. Besides possessing the requisite experience and insight into the subtleties of these complex areas, the federal government is in the prime position to formulate the most effective regulatory scheme for e-money. Through its power to regulate banks and currency, the Congress has the resources and the proper mandate to shape the development of e-money with the appropriate legislation.[114] In addition, "the nation already has federal statutes governing comparable payment systems such as electronic fund transfers and agencies experienced in drafting regulations pursuant to those laws."[115]

Furthermore, a proposal for the federal regulation of e-money has the advantage of uniformity;[116] "the public and the industry look to governments to set standards and provide a foundation and a level

114. Wilson, *supra* note 38, at 690.
115. Budnitz, *supra* note79, at 1067.
116. *Id.*

playing field upon which the private sector can operate."[117] Similarly, courts and lawyers always need rules so that they can resolve disputes as they arise in new areas.[118] Fortunately, the federal government, through the enactment of a comprehensive codification of rules, is well equipped to provide this type of guidance for the new payment devices.[119] In addition, as with other payment systems, the administrative and governmental controls established under the proposal can be expected to be the least costly method of attacking the particular problems associated with e-money systems.[120] Espousing support for this basic idea, one scholar added that

> [I]t is far easier to change the law on the federal level rather than to seek changes in every state. Therefore, if future technological developments or unforeseen consumer or industry problems necessitate amendments to the statute, these amendments can be made more quickly and in a uniform manner.[121]

Overall, by empowering the federal government to set the regulatory standards for e-money in the United States, the proposed approach gives us confidence that we are putting ourselves in a good position to move forward intelligently on the issues of e-money and money laundering.

VI. CONCLUSION

The federal government has an important choice to make in the near future. On the one hand, e-money products have only just begun to take their place in the American economy as an alternative form of currency. The products themselves have not yet reached their full development and as such they do not currently represent a substantial threat to anti-money laundering efforts in this country. Taken together, these factors make a persuasive case for the U.S. government to continue their "wait and see" approach before imposing any regulatory framework onto the various e-money systems being proposed. On the other hand, this paper has tried to argue that we have arrived at the critical stage when the Government must act to regulate this emerging industry, in order to limit the significant threats that e-money poses to the prevention of money

117. FATF PAPER, *supra* note 35, annex at para 42.
118. *See* Maggs, *supra* note 87, at 768.
119. *See id.* at 798.
120. *See* COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS, *supra* note 63, at 23.
121. Budnitz, *supra* note 79, at 1067.

laundering in this country. Moreover, the government currently possesses the knowledge, the resources and the experience to carry this out in the most effective way.

Considering that what is at stake is the potential explosion of money laundering efforts in this country, and thus a decisive blow to law enforcement's long-standing efforts to eliminate the lifeblood of criminal organizations, the Government would be wise to act now rather than waiting until problems occur. One thing is for sure: whichever posture the federal government chooses to adopt, it is certain to have lasting effects of some form or another on the e-money industry, American consumers, and perhaps even criminal money launderers.