DIGITAL CURRENCIES AND THE FINANCING OF TERRORISM

By: William Hett*

Cite as: William Hett, *Digital Currencies and the Financing of Terrorism*, XV RICH. J.L. & TECH. 4 (2008), http://law.richmond.edu/jolt/v15i2/article4.pdf.

I. INTRODUCTION

[1] Informal money transfers present a significant challenge to combating the financing of terrorist organizations worldwide. Although the U.S. and other governments have implemented measures to restrict terrorist financing, these measures were designed to regulate formal financial institutions. Accordingly, those seeking to avoid detection have turned to other methods of transferring money, such as commodities trades, *hawala*,[1] and digital currencies.[2] Many terrorist operations do not require large sums of money, making the detection and prevention of even modest transfers important. For example, the September 11 Commission estimated the cost of carrying out the 1998 U.S. embassy bombings, which

* William Hett earned his J.D. at the University of Iowa College of Law.

[1] *Hawala* refers to an ancient system of transferring money that originated in South Asia. The system is based on communications between individuals in different regions. A user gives cash to a *hawala* dealer in one place who then calls a friend or acquaintance in the destination city with instructions to pay cash to a named recipient. The system generally keeps no record of individual transactions. Instead, dealers keep track of total balances owed by one another, which could include multiple transactions back and forth over a significant period of time. PATRICK M. JOST & HARJIT SINGH SANDHU, INTERPOL GEN. SECRETARIAT, THE HAWALA ALTERNATIVE REMITTANCE SYSTEM AND ITS ROLE IN MONEY LAUNDERING (2000), http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/hawala/default.asp.

[2] Todd M. Hinnen, *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet*, 5 COLUM. SCI. & TECH. L. REV. 5, 3-4 (2004).

killed 224 people in East Africa,[3] at only $10,000.[4] Al Qaeda funded the October 18, 2002 bombing in Bali for around $20,000,[5] killing 202,[6] and the 2004 Madrid train bombings cost approximately $70,000,[7] killing 191.[8] The London bombings of July 7, 2005 were estimated to have cost several hundred to 8000 pounds sterling (up to $15,600)[9] and killed 52.[10] Even large-scale attacks with high levels of devastation are within reach of a well-financed terrorist group. The September 11, 2001 attacks in the United States were relatively inexpensive to carry out at an estimated $400,000 to $500,000,[11] killing approximately 3,007 people.[12] The low financial cost of carrying out these deadly attacks necessitates a focus on both traditional and non-traditional methods of transferring funds.

[2] The availability and popularity of digital currencies and online payment processing systems have dramatically increased in recent years.[13]

---

[3] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 70 (2004), http://www.9-11commission.gov/report/911Report.pdf.
[4] Laura K. Donohue, *Anti-Terrorist Finance in the United Kingdom and United States*, 27 MICH. J. INT'L L. 303, 305 (2006).
[5] JOHN ROTH, DOUGLAS GREENBURG & SERENA WILLE, NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, MONOGRAPH ON TERRORIST FINANCING: STAFF REPORT TO THE COMMISSION 27-28 (2004), *available at* http://www.9-11commission.gov/staff_statements/911_terrfin_monograph.pdf.
[6] *Four Sentenced for Killing Christians*, HOUSTON CHRON., Dec. 12, 2007, at A19.
[7] *Factbox-The Madrid Train Bombings and What Happened Next*, REUTERS NEWS, Feb. 14, 2007.
[8] *The Madrid Bomb Trials: Historic Verdicts*, THE ECONOMIST, Nov. 3, 2007, at 60.
[9] SIOBHAN O'NEIL, DOMESTIC SOCIAL POLICY DIVISION, CRS REPORT FOR CONGRESS, TERRORIST PRECURSOR CRIMES: ISSUES AND OPTIONS FOR CONGRESS 4 (2007), *available at* http://www.fas.org/sgp/crs/terror/RL34014.pdf.
[10] *Some Recent Terror Attacks and Plots*, SEATTLE TIMES, Sept. 6, 2007, at A12.
[11] Donohue, *supra* note 4, at 305.
[12] Data based on numbers collected from the National Consortium for the Study of Terrorism and the Responses to Terrorism. National Consortium for the Study of Terrorism and the Responses to Terrorism, Global Terrorism Database, http://www.start.umd.edu/data/gtd (follow "GTD2" hyperlink; then select "Browse by Date" and insert 09/11/2008; then select "Browse by Country" and insert "United States of America") (last visited Nov. 17, 2008).
[13] *See* Catherine Holahan, *Policing Online Money Laundering: The Financial Action Task Force Is Developing Recommendations for International Regulations to Combat Financial Cybercrime*, BUS. WK., Nov. 6, 2006, http://businessweek.com/print/technology/content/nov2006/tc20061106_986949.htm (stating PayPal alone processed $9.1 billion in the final quarter of 2006).

Some of the services currently in operation include Paypal, e-gold, Liberty Reserve, GoldMoney, V-Cash, 1mdc, Webmoney, IntGold, Stormpay, e-Dinar, cashU, and BankServ.[14] Some of these services require only a valid e-mail address to initiate an account, with the names and locations of the actual users unknown (or fabricated).[15] Although anonymous money transfer services may offer opportunities for legitimate businesses to exchange payments with customers worldwide, they also provide an extremely useful tool for drug traffickers and terrorist organizations to transfer money with a lower risk of detection.

[3] Because of the new and unique nature of these digital currencies, transfers are largely unregulated and are not subject to the same requirements as most financial institutions.[16] Normally, transfers by financial institutions are subject to a strict regulatory regime, which includes maintaining customer identification records, filing Suspicious Activities Reports (SARs), mandatory reporting on currency transfers of $10,000 or greater, and "know your customer" requirements.[17] Many digital currency providers require no customer identification and have little capability or desire to detect or report suspicious activities.[18] For this reason, such services offer opportunities for terrorist organizations to transfer money without the risks of using traditional financial institutions.

---

[14] *See, e.g.*, Paypal, https://www.paypal.com (last visited Nov. 11, 2008); e-gold, http://www.e-gold.com (last visited Nov. 11, 2008); Liberty Reserve, http://www.libertyreserve.com/en (last visited Nov. 11, 2008); GoldMoney, http://goldmoney.com (last visited Nov. 11, 2008); V-Cash, http://v-cash.com (last visited Nov. 11, 2008); 1mdc, http://www.icegold.com/1mdc.php (last visited Nov. 11, 2008); WebMoney, http://www.wmtransfer.com (last visited Nov. 11, 2008); IntGold, http://www.aboutus.org/Intgold.com (last visited Nov. 11, 2008); StormPay, http://www.stormpay.com (last visited Nov. 11, 2008); e-dinar, http://www.e-dinar.com (last visited Nov. 11, 2008); CashU, http://www.cashu.com (last visited Nov. 11, 2008); BankServ, http://www.bankserv.com (last visited Nov. 11, 2008).

[15] *See, e.g.*, Hinnen, *supra* note 2, at 33; *see also* e-gold, http://www.e-gold.com/unsecure/qanda.html (last visited Nov. 17, 2008) (stating that "there is no credit check" to open an e-gold account).

[16] *See Reform Requirements for Reporting Cash Transactions: Hearing on H.R. 5341 Before the Subcomm. on Financial Institutions and Consumer Credit*, 109th Cong. (2006) (statement of Kevin A. Delli-Colli, Deputy Assistant Director, Office of Investigations, U.S. Department of Homeland Security).

[17] *See* Donohue, *supra* note 4, at 372 (discussing some of these anti-terrorism regulations).

[18] *See* Delli-Colli, *supra* note 16.

[4] True, digital currency providers operating in the U.S. have recently experienced heightened scrutiny and now face the prospect of tighter regulation. In April 2007, the U.S. government indicted e-gold on charges of money laundering, conspiracy, and operating an unlicensed money-transmitting business.[19] The e-gold case highlights that U.S. regulations were not designed with digital currencies in mind.[20] The e-gold defendants made plausible arguments that at least parts of their operation should not be not subject to the current regulatory regime.[21] If the regulations are left unchanged, other digital currency providers could possibly tailor their operations to be exempt from the regulations that govern other financial institutions.

[5] U.S. regulation and prosecution alone cannot address the worldwide reach of these digital currencies. Many digital money services maintain their operations outside U.S. jurisdiction. For example, CashU is operated by Maktoob, Inc. in Jordan.[22] Although some transfers channeled through banks and currency exchanges in the United States would likely be subject to U.S. regulation, many would not, and some of these exchangers offer cash card services redeemable at ATMs worldwide, including in the United States.[23] Asserting jurisdiction for regulation of such exchanges is a major problem, as it is with Internet gambling.[24] Thus, continued

[19] Indictment at 1, United States v. E-gold, Ltd. et al., 550 F. Supp. 82 (D.D.C. Apr. 24, 2007) (No. 07-109), *available at* http://www.usdoj.gov/criminal/ceos/Press%20Releases/DC%20egold%20indictment.pdf [hereinafter e-gold Indictment]; *see also* Brian Doherty, *Testing Medal: The DOJ Targets E-gold*, REASON MAG., Aug. 1, 2007, *available at* http://www.reason.com/news/printer/120955.html (stating that a grand jury indicted e-gold's enterprise, parent company, and three officers).

[20] *See infra* Part III.B.

[21] Memorandum of Law in Support of Defendants' Motion to Dismiss Counts Two, Three and Four of the Indictment at 13-14, United States v. E-gold Ltd., 550 F. Supp. 82 (D.D.C. Feb. 11, 2008) (No. 07-109) [hereinafter Memorandum of Law in Support of Defendants' Motion to Dismiss].

[22] Maktoob Group, About Us, http://www.maktoobgroup.com/inside.htm (last visited Nov. 17, 2008).

[23] *See, e.g.*, Cash Cards International, http://www.cashcards.net/rep/99152/home_page_text.html (last visited Nov. 17, 2008).

[24] *See* Ronnie D. Crisco, Jr., Comment, *Follow the Leaders: A Constructive Examination of Existing Regulatory Tools That Could Be Applied to Internet Gambling*, 5 N.C. J.L. & TECH. 155, 158 (2003) ("[t]he majority of Internet gambling businesses are located in tax-havens like Antigua and Belize that impose virtually no formal restrictions on these

International efforts are essential and will be carried out by organizations such as the Financial Action Task Force (FATF).[25]

[6] This article begins by describing the nature of digital currencies, how they work, and how a terrorist operation might use transfers of value through a digital currency to access usable cash in the United States or other target countries. Part II discusses the current U.S. legislative and regulatory framework of financial institutions and how digital currency providers fit into this regime. Part III examines the enforcement of U.S. regulations, specifically the e-gold prosecution and the use of 18 U.S.C. § 1960 to prosecute unlicensed money transmitting businesses. Part IV discusses the future of digital currencies in the United States and the effects of prosecutions like the e-gold case on those businesses. Finally, Part V examines the problems of the current regulatory regime and the challenge of regulating digital currencies outside U.S. jurisdiction. The article proposes that in order to better protect against the risks posed by digital currencies, the United States should consider the following measures: (1) specifically include both digital currency providers and digital currency exchangers in the regulations defining a "money services business" to subject them to regulation as "financial institutions"; (2) create due diligence requirements for currency exchangers that accept digital currencies for the purchase of ATM cash and debit cards, with the degree of customer identification and verification procedures increasing for purchases and transfers of higher values; (3) place specific per day and per year value limits on purchases of cash cards with digital currencies, and limits on the number of cash cards that each individual may purchase; and (4) prohibit U.S. banks and card system networks from processing ATM/debit payment requests from digital currency exchangers located abroad that deal in digital currencies.

---

enterprises."); *cf.* Adrian Parke & Mark Griffiths, *Why Internet Gambling Prohibition Will Ultimately Fail*, 8 GAMING L. REV. 295, 296-97 (2004) (stating that it is difficult to differentiate between legal and illegal data transfers when monitoring online gambling and that many transfers are to Internet gambling providers registered in countries with limited restrictions).

[25] *See infra* text accompanying note 43.

A. HOW DIGITAL CURRENCIES WORK

[7] Digital currencies function as an online exchange medium by allowing transfers of value without the use of hard currency or electronic banking channels.[26] One of the rationales for using a digital currency is "to facilitate online transactions without regard for underlying currencies or access to foreign exchange."[27] Digital currencies serve as an alternative method of exchange for those conducting transactions online with known or unknown parties.[28] These currencies are universal, sometimes tied to the exchange rates of hard metals, such as gold or silver, or other commodities.[29] The digital currency provider issues the user an account, funded through a currency exchanger that deals in the specified currency.[30] Exchangers accept cash, checks, credit cards, wire transfers, commodities, or other items of value in exchange for funding the customer's account.[31] Once funded, the customer accesses the digital currency account online and transfers the funds to another account holder located anywhere in the world.[32]

[8] Some of the existing digital currencies, or online payment processing systems, include Paypal, e-gold, Liberty Reserve, GoldMoney, V-Cash, 1mdc, Webmoney, IntGold, Stormpay, e-Dinar, Cash-U, and BankServe.[33] Each of these digital currencies varies slightly in operation. For example,

---

[26] Digital Currency is perhaps the least well-known type of Internet payment system. It can be defined as a foreign currency with value that may be exchanged back and forth with U.S. dollars but which requires clearing or settlement. A purchaser obtains funds for use on the Internet by converting funds from a bank account or a credit card into an electronic token for use on the internet. Robert F. Stankey, *Internet Payment Systems: Legal Issues Facing Businesses, Consumers and Payment Service Providers*, 6 COMMLAW CONSPECTUS 11, 22 (1998).

[27] FINANCIAL ACTION TASK FORCE, REPORT ON NEW PAYMENT METHODS 9 (2006), *available at* http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf [hereinafter FATF REPORT ON NEW PAYMENT METHODS].

[28] U.S. DEP'T OF JUSTICE, NAT'L DRUG INTELLIGENCE CTR., MONEY LAUNDERING IN DIGITAL CURRENCIES 1 (2008), *available at* http://www.usdoj.gov/ndic/pubs28/28675/28675p.pdf [hereinafter MONEY LAUNDERING IN DIGITAL CURRENCIES].

[29] *Id.* at 1-2.

[30] *See id.* at 3 & n.8.

[31] *Id.* at 3-4.

[32] *Id.* at 1.

[33] *See supra* note 14.

Paypal is tied to a bank account or a credit card and is essentially a credit card processing service.[34] Most other services, such as e-gold, require the user to load the account with money before one may "spend," or transfer, the digital currency to another account holder.[35]

[9] Those digital currencies not tied to a credit card or bank account must make use of a money exchange service that accepts a national currency in exchange for a digital currency.[36] The digital currency provider itself may provide this service, or it may prefer to leave the business of exchange to others.[37] Whether or not it provides this service itself may alter the legal requirements and regulations to which it is subject.[38] These differences will be further discussed in Parts II and III.

B. POTENTIAL FOR UNDETECTABLE TRANSFERS, MONEY LAUNDERING, FINANCING TERRORISM

[10] Digital currencies afford a mechanism for money launderers and terrorists to transfer money internationally with a lower risk of detection than transfers carried out through traditional banking channels.[39] Regulations of financial institutions, such as "know your customer" requirements and mandatory reporting for certain transactions, make the detection of illegal transfers and associated criminal activity more probable.[40] U.S. officials hinted to reporters "that e-gold is a 'PayPal' for terrorists to move cash stealthily among operatives."[41] Some digital

[34] Brian Grow et al., *Gold Rush: Online Payment Systems Like E-gold Ltd. Are Becoming the Currency of Choice for Cybercrooks*, BUS. WK., Jan. 9, 2006, at 68.
[35] E-gold enables an individual "to spend gold as money" after opening an account by wiring money to e-gold or depositing money from a bank accounts, credit cards, or a money order. *See* e-gold, *supra* note 15.
[36] *See* MONEY LAUNDERING IN DIGITAL CURRENCIES, *supra* note 28, at 2.
[37] *See* id.
[38] *See infra* Part II.B.
[39] *See* Hinnen, *supra* note 2, at 27, 33-35.
[40] See *infra* Part II, for a detailed discussion of these regulations. See Josh Meyer & Erika Hayasaki, *Bank Transactions Put Focus on Spitzer: Neither the New York Governor nor the Call-Girl Ring He Has Been Linked to Was Specifically Targeted*, L.A. TIMES, Mar. 12, 2008, at 16, for an example of how such regulations can uncover criminal activity.
[41] James Gordon Meek, *24-Karat Worry on the Web*, N.Y. DAILY NEWS, June 3, 2007, at 2.

currency providers allow users to maintain anonymous accounts.[42] For example, acquiring an e-gold account takes only minutes and includes no verification procedure, unlike the process required by banks.[43] In some instances, all that is needed to load money onto an account is a long distance phone card. [44] In addition, the existence of currency and e-gold exchangers worldwide makes it difficult to find out which trader or exchanger funded the account.[45]

[11] The Financial Action Task Force (FATF), an intergovernmental body composed of 34 member-states, compared digital currencies to physical cash in order to assess the risk of digital value transfer systems.[46] "Physical cash is often the ideal method of value transfer for criminal activity because it is anonymous, untraceable, requires no intermediary, is widely accepted, and provides for immediate settlement."[47] Therefore, a value transfer system, such as digital currency, contains a higher risk of being vulnerable to money laundering and terrorist financing activities the more closely it resembles physical cash. Using cash is anonymous and requires no verification, customer identification, or recordkeeping.[48] Physical cash also has no limit to the amount that may be spent,[49] apart from the physical barrier of carrying a quantity of cash.[50] Major currencies, such as dollars and euros, have few geographic limitations, as they can be exchanged worldwide, while others may have a narrower area of acceptance.[51]

[12] Thus, those digital currencies that verify fewer aspects of one's identity present a higher risk of being used by money launderers and terrorists, as they are more anonymous and more difficult to trace.[52]

---

[42] FATF REPORT ON NEW PAYMENT METHODS, *supra* note 27, at 9.
[43] Jeremy Au Yong, *You Can Kiss Your Money Goodbye: Net Currency System Hides Cheaters' Tracks As Users Are Anonymous and Payments Difficult to Track*, STRAITS TIMES (Sing.), Nov. 12, 2006.
[44] Holahan, *supra* note 13.
[45] *Id.*
[46] FATF REPORT ON NEW PAYMENT METHODS, *supra* note 27, at 10.
[47] *Id.* at 10 n.22.
[48] *Id.* at 10-11 tbl.2.
[49] *Id.*
[50] *Id.* at 10 n.22.
[51] FATF REPORT ON NEW PAYMENT METHODS, *supra* note 27, at 10.
[52] *See* MONEY LAUNDERING IN DIGITAL CURRENCIES, *supra* note 28, at 3-4.

Likewise, those digital currencies that have a lower threshold of customer identification and verification and either severely limit or lack recordkeeping also pose a higher risk.[53] For example, e-gold has been criticized for providing little or no verification of the identity of its users.[54] Active accounts were discovered under the names "Bud Weiser" and "Mickey Mouse," indicating that no internal checks exist to verify who is using the service.[55]

[13] In the context of money laundering or financing terrorism, digital currencies provide a flexible and potentially undetectable method for funds transfers.[56] As long as both parties to the transfer of value have accounts with the digital currency server, most digital currencies have no limits to the amount of value that may be transferred.[57] Further, there are often fewer geographical limitations to the transfer of digital currencies, because these currencies operate over the Internet.[58] Individuals may access their accounts and make transfers online from anywhere in the world. In the context of terrorism the limit is on liquidity; it is often difficult to convert digital funds into usable cash within the target country.

C. MECHANICS OF HOW DIGITAL CURRENCIES COULD FINANCE TERRORISM

[14] Using a digital currency to finance a terror attack in the United States or another target country would require several steps. Transferring physical cash or funds from a bank account in one country, to cash or usable funds in the United States, necessitates both a digital currency dealer and a currency exchanger.[59] Sometimes a digital currency provider will perform both functions if it accepts wire transfers or credit cards in order to directly fund an account.[60] Other types of digital currencies, such as e-gold, however, require the use of an independent currency or

[53] *Id.*
[54] *See* e-gold Indictment 3-4, *supra* note 19, at 12-13.
[55] Meek, *supra* note 41.
[56] *See* MONEY LAUNDERING IN DIGITAL CURRENCIES, *supra* note 28, at 4.
[57] FATF REPORT ON NEW PAYMENT METHODS, *supra* note 27, at 9-10.
[58] *See supra* notes 23-24 and accompanying text.
[59] FATF REPORT ON NEW PAYMENT METHODS, *supra* note 27, at 9.
[60] *See id.*

commodities exchanger.[61] In these cases, one must pay the exchanger via cash, check, credit card, or wire transfer, and the exchanger will then make a "spend" from its digital currency account to the customer's account.[62] The digital currency provider itself, in such a situation, only deals in exchanges of its own currency and does not deal with funds in any national currency.

[15] Examining the mechanics of a transaction at a practical level, there are at least several different methods through which one could transfer funds using a digital currency. The first step would be to use a check, credit card, wire transfer, cash or other value transfer to pay a currency exchanger that trades in digital currencies. Such dealers, or exchangers, operate in much the same way that traditional hard currency exchangers operate. The exchanger accepts payment in cash (or check or wire transfer) and for a fee, grants the customer a quantity of digital currency through a "spend" from its own account to the customer's.[63] After obtaining the digital currency, the individual is free to transfer it anonymously online to someone else, who could be anywhere in the world.

[16] The recipient may then use various methods to convert the digital currency into usable money in the United States. First, the recipient could use a currency exchanger to obtain hard currency in U.S. dollars.[64] Such exchangers in the United States, however, are subject to financial regulations, so transfers would leave a paper trail and not be completely anonymous. A second option would be to transfer the digital currency via wire transfer to a bank in another country that has fewer banking regulations and reporting requirements. Then, with an ATM card already held from the foreign bank, the individual could make purchases and obtain dollars in cash. This method, however, would also leave a trail, as withdrawing funds in the United States would reveal at least the account holder's foreign bank, which is likely to have recorded customer information and be subject to some regulation.

[61] *See infra* text accompanying notes 122-123.
[62] *See supra* note 35 and accompanying text.
[63] Au Yong, *supra* note 43; *id.*
[64] MONEY LAUNDERING IN DIGITAL CURRENCIES, *supra* note 28, at 2.

[17] A third option would be to purchase cash cards, or gift cards, which are prepaid cards that function like debit or ATM cards. Several exchangers provide a service of accepting digital currencies and exchanging them for a national currency loaded onto an ATM card.[65] These cards are generally independent from banks or credit cards, even though they may be associated with a card payment network such as MasterCard or Visa.[66] The only thing required to load money onto an account in some cases is a long-distance phone card.[67] A customer can opt to receive a cash card via international courier and then withdraw or spend the funds at any ATM or vendor that accepts MasterCard and Visa.[68] Most such cards are reloadable.[69] The most common digital currency accepted by these service providers is e-gold.[70] The level of regulation to which these new entities are subject in their home countries is uncertain. In one reported case, an individual purchased more than 300 prepaid cards in order to launder $2 million from the United States to Colombia.[71]

[18] Digital currency exchangers that issue cash or debit cards appear to require customers to provide only minimal personal information, such as names, addresses, and phone numbers.[72] The extent to which these providers verify this information is unknown. In addition, although ATM withdrawals leave an electronic trail, the cardholder and origin of the funds may be untraceable if the card provider is not subject to U.S. regulations or if what little information it has is forged or unverified.[73]

---

[65] *See, e.g.*, Cash Cards International, *supra* note 23; Express Cash Card, https://www.exprescash.com/default.aspx (last visited Nov. 18, 2008); E-Forexgold, https://www.e-forexgold.com/efx2/debit_cards (last visited Nov. 18, 2008); Digital Wealth Global Debit Cards, http://www.dwgcard.com/index.php (last visited Nov. 18, 2008).

[66] *See* FATF REPORT ON NEW PAYMENT METHODS, *supra* note 27, at 4.

[67] Holahan, *supra* note 13.

[68] FATF REPORT ON NEW PAYMENT METHODS, *supra* note 27, at 4.

[69] *Id.*

[70] *Id.* at 9.

[71] *Id.* at 12.

[72] *See, e.g.* GoldMoney, https://secure.goldmoney.com/user/opnhld.php (last visited Nov. 21, 2008); LibertyReserve, https://www.libertyreserve.com/en/signup/step1/index.aspx (last visited Nov. 21, 2008); LutLot, http://www.lutlot.com/lutlot/user/user_register.php (last visited Nov. 21, 2008); V-Cash, http://v-cash.com/rep/54165/create.html (last visited Nov. 21, 2008); Webmoney, https://start.wmtransfer.com/signup.aspx?lang=en (last visited Nov. 21, 2008).

[73] *See id.* at 11.

Such "open-system, prepaid cards" as termed by a FATF report, contain a higher risk for use in money laundering or terrorist-financed operations if not mitigated by account or transactional limitations.[74]

[19] The providers of debit and cash cards loadable with e-gold or other digital currencies are often incorporated in countries notorious for weak or insufficient financial regulations. For example, Cash Cards International is incorporated in St. Kitts,[75] and E-Bullion Debit Cards and E-forexgold are incorporated in Panama.[76] FATF included St. Kitts on its list of Non-Cooperative Countries and Territories (NCCT) until 2002.[77] Panama was included as a NCCT until 2001.[78] Although these countries have made progress in financial regulations through recent lawmaking, downstream enforcement of these stricter regulations for financial institutions remains uncertain.

[20] The existence of these digital currency providers and exchangers outside the United States presents a higher risk than traditional transfers through bank accounts via wire transfers or ATM withdrawals. The location of these providers means that it may be impossible for U.S. law enforcement to access account information under circumstances that would allow an administrative subpoena or search warrant within the United States.[79] Tracking the sources of funds channeled through digital currencies and exchangers of these currencies is thus extremely difficult, if not impossible.

[21] The challenges involved with digital currency providers and exchangers located outside the United States are further discussed in Part VI. The following section examines the current U.S. regulatory regime for

---

[74] *Id.*
[75] Cash Cards International, *supra* note 23.
[76] *Century City*, CITY NEWS SERVICE (Los Angeles), July 30, 2008; E-Forexgold, *supra* note 55.
[77] FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING, ANNUAL REVIEW OF NON-COOPERATIVE COUNTRIES OR TERRITORIES 16 (2003), *available at* http://www.fatf-gafi.org/dataoecd/4/30/33922392.PDF [hereinafter FATF ON MONEY LAUNDERING].
[78] FINANCIAL ACTION TASK FORCE, REVIEW TO IDENTIFY NON-COOPERATIVE COUNTRIES AND TERRITORIES: INCREASING THE WORLD-WIDE EFFECTIVENESS OF ANTI-MONEY LAUNDERING MEASURES 19 (2002), *available at* http://www.fatf-gafi.org/dataoecd/4/32/33922320.pdf.
[79] Crisco, *supra* note 24.

financial institutions. It begins by discussing the overall goals of regulation. It then briefly outlines the history of regulations in the United States and discusses key elements of the regulatory regime.

II. DOMESTIC REGULATION OF FINANCIAL INSTITUTIONS AND DIGITAL CURRENCY PROVIDERS

A. GOALS OF FINANCIAL REGULATION

[22] One may wonder why digital currency transactions, even if more anonymous than other transfers, present a greater threat to the security of the United States and other target countries. After all, most wire transfers and withdrawals from bank accounts in the United States that arouse suspicion are not halted. They merely trigger reporting requirements. Thus, the damage, if any, is already done with the act of the transfer itself. But even if regulation of these traditional financial exchanges does not always prevent the actual funds transfer, regulation also serves another purpose: aiding investigations.

[23] One major goal of financial regulation is to detect and prevent the financing of terrorism, which means preventing potential terrorists in the United States (or other targeted countries) from obtaining physical cash or any other method of funding that allows them to carry out attacks.[80] Even with a stricter regulation regime than is currently in place in the United States, however, preventing all such transfers is likely to prove impossible.[81] Indeed, the stricter regulations now in place, such as those requiring financial institutions to file Suspicious Activities Reports for a wider variety of activity, would not be able to detect the financial transfers that were made by the 9/11 hijackers.[82] For this reason, regulation has a "dual purpose," including detection and prevention as well as aiding investigation after the commission of a crime.[83]

[80] Donohue, *supra* note 4, at 304-05.
[81] *See id.* at 304.
[82] *Id.* at 396.
[83] *Id.* at 374.

B. U.S. REGULATION OF DIGITAL CURRENCY PROVIDERS AND EXCHANGERS

[24] There is some ambiguity as to how digital currency providers, and exchanges dealing in such currencies, fit into the U.S. regulatory scheme. One source of confusion is that the relevant statutes and regulations contain differing and sometimes conflicting definitions of key terms. For example, 31 U.S.C. § 5312 defines "financial institution" differently than the regulations at 31 C.F.R. § 103.11. The statute lists twenty-six categories of "financial institutions," while the regulations break them down into nine categories. [84] In the case of digital currencies, the differences in the definitions would not likely produce differing results. That is, if a digital currency is a "financial institution" for the purposes of the regulations, it is also likely to be a "financial institution" under the statute. Both definitions include a category of any "person engaged as a business," in either the statutory "transmission of funds" [85] or regulatory "transfer of funds."[86]

---

[84] 31 U.S.C. § 5312(a)(2) (2006); 31 C.F.R. § 103.11(n) (2008).

[85] The statutory definition of "financial institution" includes:

> (R) a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system.

31 U.S.C. § 5312(a)(2)(R).

[86] The regulatory definition of "financial institution" in 31 C.F.R. § 103.11(n) includes the term "money services business," which is defined as a:

> (5) Money transmitter –
> (i) In general. Money transmitter:
> (A) Any person, whether or not licensed or required to be licensed, who engages as a business in accepting currency, or funds denominated in currency, and transmits the currency or funds, or the value of the currency or funds, by any means through a financial agency or institution, a Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System, or both, or an electronic funds transfer network; or
> (B) Any other person engaged as a business in the *transfer of funds.*

[25] If digital currency providers are to be subject to the regulatory regime, they must fall within the "money transmitter" category as "any other person engaged . . . in the transfer of funds."[87] The regulations state that the determination of whether an entity falls into the category of a "money transmitter" will depend on the facts and circumstances.[88] This limitation also suggests that the mere acceptance or transfer of funds to settle accounts pursuant to a transaction itself will not generally subject an individual or entity to the regulations.[89] Some have argued that this limitation could be used as a defense by digital currency providers,[90] although the meaning of the limitation in 31 C.F.R. § 103.11(uu)(5)(ii) remains unclear as it has not yet been addressed by courts or regulatory agencies.

[26] Assuming a digital currency provider qualifies as a "financial institution," various reporting and recording obligations apply. The Bank Secrecy Act[91] imposes several such obligations. In its own words, the statute requires financial institutions to maintain "certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism."[92] The Act's justification is rooted in the idea that private industry, rather than government, is better able to detect illegal or suspicious uses of financial institutions.[93] The statute requires financial institutions to maintain certain information regarding account owners, fund sources, and whether transactions are consistent with customer profiles.[94]

---

31 C.F.R. § 103.11(uu) (emphasis added).
[87] 31 U.S.C. § 5312(a)(2)(R); 31 C.F.R. §§ 103.11(n)(3), (uu)(5)(i)(B).
[88] 31 C.F.R. § 103.11(uu)(5)(ii).
[89] *Id.*
[90] Sarah Jane Hughes et al., *Developments in the Law Concerning Stored-Value Cards and Other Electronic Payments Products*, 63 BUS. LAW., 237, 262 (2007).
[91] 31 U.S.C. § 5311 (2006).
[92] *Id.*
[93] Donohue, *supra* note 4, at 356-57.
[94] *Id.* at 357.

[27] The USA PATRIOT Act, passed in October of 2001,[95] imposes further measures in an attempt to detect suspicious or illegal movements of funds for the purpose of combating international terrorism.[96] The Act requires the U.S. Treasury Department to promulgate regulations with a minimum level of customer identification measures.[97] The USA PATRIOT Act includes enhanced "know your customer" rules that require financial institutions, at a minimum, to implement "reasonable procedures" to verify the identity of those seeking to open accounts, and to maintain records of information collected, including name, address, and other identifying information.[98] The USA PATRIOT Act also requires all financial institutions to implement anti-money laundering programs.[99] Regulations list requirements that specifically apply to "money services businesses," including among other things, procedures for verifying customer identification, filing reports, creating and retaining records, and responding to law enforcement requests.[100]

1. SUSPICIOUS ACTIVITIES REPORTS FOR MONEY SERVICES BUSINESSES

[28] As discussed above, if digital currency providers and exchangers are to fall under the regulatory regime, it is in the "money services business" category. Regulations require "money services businesses" to file a suspicious activities report (SAR) with the U.S. Treasury Department for any transaction involving aggregate funds of $2000 where the "money services business" knows or has reason to know that the transaction "involves funds derived from illegal activity"; "is designed to evade" reporting requirements or other regulations; "serves no business or apparent lawful purpose"; or "involves [the] use of the money services

[95] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 31 U.S.C.).
[96] Robert M. Taylor, III, *Anti-Money Laundering and Anti-Terrorist Financing Requirements Applicable to Financial Institutions*, 120 BANKING L.J. 497, 499 (2003).
[97] 31 U.S.C. § 5318 (2006).
[98] *Id.* § 5318(l)(1)-(2); Taylor, *supra* note 96.
[99] *Id.* § 5318(h)(1).
[100] 31 C.F.R. § 103.125(d)(1)(i) (2008).

business to facilitate criminal activity."[101] The SAR must be filed within thirty days of detecting the suspicious activity.[102]

2. RECORDKEEPING REQUIREMENTS FOR ALL FINANCIAL INSTITUTIONS

[29] Regulations require all financial institutions to retain records for five years when they are for certain transactions in excess of $10,000 including records of advice, requests, or instruction in any transaction that results in, or intends to result in, the transfer of currency or other monetary instruments, funds, checks, investment securities, or credit, as well as fund transfers that equal or exceed $3,000.[103] "Additional record-keeping requirements apply specifically to banks, securities brokers and dealers, casinos, and currency dealers and exchangers."[104] The regulations require non-bank financial institutions to retain records for transactions in the amount of $3,000 or more.[105] For each transfer, non-bank financial institutions must record the following: the name and address of the transmitter, the amount of the transfer, the date, the identity of the recipient's institution, and if available, the recipient's name, address, account number, and identifying information.[106]

[30] In addition, non-bank financial institutions with branches or agents located in the United States must retain further information for transactions in the amount of $3,000 or more conducted by individuals who are anyone other than "established customers."[107] Regulations define an "established customer" as a person with an account for which the financial institution maintains a file on the name, address, and taxpayer identification number (social security number, alien registration number, or passport number and country of issuance).[108] If a person is not an "established customer," the regulations require that the financial

[101] *Id.* § 103.20(a)(2)(i)-(iv).
[102] *Id.* § 103.20(b)(3).
[103] *Id.* § 103.33(a)-(d); *see also* Andrew Chung & John Mack, *Financial Institutions Fraud*, 44 AM. CRIM. L. REV. 555, 585-86 (2007) (discussing the record-keeping requirements under the Bank Secrecy Act, 31 U.S.C. § 5311 (2006)).
[104] Chung & Mack, *supra* note 103, at 586.
[105] 31 C.F.R. § 103.33(f).
[106] *Id.* § 103.33(f)(1)(i).
[107] *Id.* § 103.33(f)(2).
[108] *Id.* § 103.11(l).

institution collect and record this information before carrying out the transfer.[109]

3. ADDITIONAL REQUIREMENTS FOR MONEY SERVICES BUSINESSES

[31] The regulations further specify requirements for money services businesses. [110] Financial institutions in this category, which likely include many digital currency providers and exchangers, must initially register with the Financial Crimes Enforcement Network (FinCEN) of the Treasury Department and renew the registration every two years.[111] Each money services business must also submit a list of its agents, as required by 31 U.S.C. § 5330.[112] This is in addition to the obligations of all financial institutions, such as the "know your customer" requirements and those which require institutions to maintain additional records of identifying information for accounts involving transactions of $3,000 or more.[113]

[32] The jurisdictional requirement that the financial institution, or its offices, branches, or agents be located in the United States limits the reach and effectiveness of the regulations, especially in the context of digital currency providers.[114] As noted above, many such businesses are specifically located in foreign locales that lack stringent recordkeeping requirements. A customer in the United States can conduct transactions online through exchangers who deal in digital currencies, completely avoiding the recording of account or transactional information, and thus remaining anonymous.[115] Even with a wire transfer into a U.S. bank or an ATM withdrawal within the United States, the trail of the funds' source quickly dries up at the foreign digital currency exchanger's doorstep.

---

[109] *Id.* § 103.33(f)(2)-(3).
[110] *See generally id.* § 103.41 (2008) (discussing registration requirements for money services businesses).
[111] *Id.* § 103.41(b)(1)-(2).
[112] *Id.* § 103.41(a)(1).
[113] *See id.* § 103.33 (e); *see also* Donohue, *supra* note 4, at 357 (discussing how the statute minimizes exposure to risk by requiring banks to "know" their customers).
[114] 31 C.F.R. § 103.33(e).
[115] *See generally* Hinnen, supra note 2, at 1, 4-9 (explaining how the Internet can be used to make anonymous transactions); MONEY LAUNDERING IN DIGITAL CURRENCIES, *supra* note 28.

4. PENALTIES FOR VIOLATIONS OF REPORTING REQUIREMENTS AND REGULATIONS

[33] For those subject to U.S. jurisdiction, violations of the statutory or regulatory reporting requirements are punishable by either a maximum five-year imprisonment or a maximum $250,000 fine, or both.[116] In addition, such violations are also chargeable offenses under the federal prong of the unlicensed money transmitting business statute, 18 U.S.C. § 1960.[117] The statute defines "unlicensed money transmitting business" in three ways: (A) operation of a money transmitting business without a state license where the state requires it;[118] (B) failure to comply with the money transmitting business registration requirements under 31 U.S.C. § 5330 or the accompanying regulations;[119] or (C) transmitting funds knowing that they are derived from a criminal offense or are intended to promote unlawful activity.[120] The Code carries a maximum punishment of a five-year imprisonment.[121]

[34] In order to be subject to prosecution under the federal licensing prong of 18 U.S.C. § 1960(b)(1)(B), a digital currency provider or exchanger is subject to the registration requirements of 31 U.S.C. § 5330 if it qualifies as a "money transmitting business," which is any business providing currency exchange, money transmitting services, or anyone who "engages as a business in the transmission of funds."[122] Thus, the language tracks the definition of a "money services business," defined by 31 C.F.R. §103.11(n) and (uu). If a digital currency provider or exchanger falls into this category, then failure to register with the U.S. Treasury

[116] 31 U.S.C. § 5322(a) (2006).
[117] John D.G. Waszak, *The Obstacles to Suppressing Radical Islamic Terrorist Financing*, 37 CASE W. RES. J. INT'L L. 673, 686 (2005). *See generally* Courtney J. Linn, *One-Hour Money Laundering: Prosecuting Unlicensed Money Transmitting Businesses Under 18 U.S.C. § 1960*, 8 U.C. DAVIS BUS. L.J. 138 (2007).
[118] 18 U.S.C. § 1960(b)(1)(A) (2006). The constitutionality of 18 U.S.C. § 1960(b)(1)(A) was called into question in *United States v. Barre*, 313 F. Supp. 2d 1086, 1090-91 (D. Colo. 2004).
[119] 18 U.S.C. § 1960(b)(1)(B).
[120] *Id.* § 1960(b)(1)(C).
[121] *Id.* § 1960(a).
[122] 31 U.S.C. § 5330(d)(1)(A) (2006).

Department appears to be a chargeable offense for an unlicensed money transmitting business.[123]

III. APPLICATION OF REGULATIONS TO DIGITAL CURRENCY PROVIDERS, CURRENCY EXCHANGERS

[35] The U.S. Justice Department is exploring the bounds of enforcing this statutory and regulatory regime, evidenced by its bringing charges against at least one digital currency provider.[124] Those in charge of operating the digital currency provider e-gold have recently come under increased scrutiny.[125] To date, this is the only digital currency provider or exchanger to face serious forfeitures and criminal charges. The e-gold case serves as an example of how the government interprets the regulations (in light of their statutory basis) and who is subject to them.[126] In addition, it brings certain defenses to light that defendants are likely to raise in such cases. This section uses the e-gold example as a case study to better understand how the United States will seek to enforce the regulations against digital currency providers and exchangers.

A. VIOLATIONS OF REGULATIONS, PROSECUTIONS OF DIGITAL CURRENCY PROVIDERS, E-GOLD CASE

[36] On April 24, 2007, e-gold, Ltd., Gold & Silver Reserve, Inc. and founders Dr. Douglas L. Jackson, Reid A. Jackson, and Barry K. Downey were indicted for money laundering, conspiracy, and operating an unlicensed money transmitting business.[127] On July 21, 2008, the U.S. Department of Justice announced that each defendant pleaded guilty to

[123] *See id.* § 5312(a)(2)(R) (stating that "any other person who engages as a business in the transmission of funds" may qualify as a financial institution); *see* 31 C.F.R. §§ 103.11(uu)(5)(i)(A)-(B) (2008).
[124] Press Release, U.S. Dep't of Justice, Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting (Apr. 27, 2007), *available at* http://www.usdoj.gov/opa/pr/2007/April/07_crm_301.html.
[125] E-gold Indictment, *supra* note 19, at 1-2.
[126] *See generally id.* (describing the elements of the charges brought against e-gold).
[127] E-gold Indictment, *supra* note 19, at 16; Press Release, U.S. Dep't of Justice, *supra* note 124.

one or more of the charges.[128] The discussion in this article focuses on the charge of operating an unlicensed money transmitting business under federal law, pursuant to 18 U.S.C. § 1960. The statute criminalizes operation of a money transmitting business without a license (in jurisdictions where state law requires a license) and operation without proper federal registration.[129] The e-gold indictment contains counts alleging violations of both the state and federal licensing prongs.[130]

[37] The general elements of the offense under the state licensing prong are: 1) operation of a money transmitting business; 2) that affects interstate or foreign commerce; 3) that is unlicensed under state law; 4) operating in a state that requires a license for such operation; 5) where the state punishes such unlicensed operation.[131] Under the federal prong, the statute requires the same two first elements, and also requires that the operation fail to comply with the registration requirements under 31 U.S.C. § 5330 or the accompanying regulations,[132] or involves the transmission of funds "that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity."[133]

[38] For an understanding of the e-gold case, it is necessary to understand the distinction between a digital currency provider and a digital currency exchanger. The digital currency provider maintains the online currency system and handles transactions between accounts online.[134] The digital currency exchanger accepts national currencies and multiple payment methods and issues users a quantity of the digital currency, usually for an exchange fee.[135] In practice, however, these roles sometimes overlap, as in the case of the e-gold defendants. The e-gold digital currency provider

[128] *Digital Currency Business E-gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges*, U.S. FED. NEWS, July 21, 2008, *available at* 2008 WLNR 13724535.
[129] 18 U.S.C. § 1960(b)(A)-(C) (2006).
[130] E-gold Indictment, *supra* note 19, at 25-26.
[131] U.S. v. Talebnejad, 460 F.3d 563 (4th Cir. 2006).
[132] 18 U.S.C. § 1960(b)(1)(B).
[133] *Id.* § 1960(b)(1)(C).
[134] MONEY LAUNDERING IN DIGITAL CURRENCIES, *supra* note 28, at 2.
[135] *Id.*

is e-gold, Ltd., incorporated in Nevis,[136] which handles the "roles of issuance and settlement."[137] The e-gold system makes use of independent currency exchangers, although the parent corporation Gold & Silver Reserve, Inc., a Delaware corporation headquartered in Melbourne, Florida,[138] also operates its own currency exchange called OmniPay, described as "the primary source for e-gold exchange."[139] OmniPay is not currently operational after the 2007 indictment; its website indicates its intent to suspend new account registrations until it has complied with applicable federal and state regulations.[140]

[39] Gold & Silver Reserve was in exclusive control of the e-gold digital currency system from 1996 through 1999.[141] In January of 2000, however, the issuance and settlement roles were transferred to e-gold, Ltd. in order "to further assure e-gold's freedom from default risk and finality of settlement by dissociating the e-gold Issuer from business risks relating to exchange."[142] This was also likely a strategic move in an attempt to avoid becoming subject to the regulatory regime of financial institutions in the United States.

[40] E-gold, Ltd. now operates the digital currency system, whereby accountholders may exchange values with each other, measured in weights of gold.[143] The system purportedly holds a fixed quantity of gold bullion at storage repositories "certified by the London Bullion Market Association,"[144] and the user agreement states that e-gold "is payable to User, fine gram for gram, on demand, in physical gold."[145] Title to the gold bullion is held in trust by e-gold Bullion Reserve Special Purpose Trust, and the bullion may not be liquidated without the signatures of both

[136] Nevis is located in the Caribbean Sea, near the island of Saint Kitts. *See* https://www.cia.gov/library/publications/the-world-factbook/geos/sc.html.
[137] OmniPay, About Us, http://www.omnipay.com/aboutus.asp (last visited Nov. 18, 2008).
[138] *Id.*
[139] OmniPay, https://www.omnipay.com/default.asp (last visited Nov. 18, 2008).
[140] OmniPay, http://www.omnipay.com/opa2007.asp (last visited Nov. 18, 2008).
[141] *See* OmniPay, About Us, *supra* note 137.
[142] *Id.*
[143] E-gold, *supra* note 15.
[144] *Id.*
[145] E-gold Account User Agreement § 3.1.1, http://www.e-gold.com/unsecure/e-g-agree.htm (last visited Nov. 18, 2008).

e-gold, Ltd. and a third party escrow agent.[146] Account holders "spend" e-gold by transferring values to other account holders through transactions ordered online.[147] These transactions are irreversible.[148] The e-gold website states that e-gold, Ltd.. does not possess any national currency or bank account.[149] Yet, to recover bullion storage costs, e-gold apparently charges "Agio fees" and "spend fees"; the latter are deducted in e-metal.[150] It is unclear how e-gold extracts this fee to pay the bullion storage facility if it does not maintain bank accounts.

[41] Transferring a national currency through e-gold to another party is at least a three step process. First, one must pay a currency exchanger that accepts e-gold a quantity of national currency, or other digital currency.[151] As mentioned above, Gold & Silver Reserve's exchanger, OmniPay, offered these services up until the indictment.[152] Currently, any exchange must be carried out by independent exchangers.[153] Second, the exchanger accepts a national currency, or other transfer of value, and issues the customer an equivalent in e-gold, minus a transactional fee.[154] The exchanger affects this transfer by issuing a "spend"[155] from its e-gold account to the account of the customer. Third, the customer is then free to transfer the e-gold as he or she sees fit to another account holder.[156] This account holder may make further transfers, or could issue a "spend" to the

[146] Defendants' Motion to Vacate Seizure Warrant and to Modify Restraining Order and Request for an Evidentiary Hearing at 20, n.19, United States v. E-gold, Ltd., 550 F. Supp. 2d 82 (D.D.C. May 17, 2007) (No. 07-109) (citing to e-gold Bullion Reserve Special Purpose Trust ¶ 4.1, *available at* http://www.e-gold.com/contracts/egold-spt-111899.htm).
[147] E-gold Account User Agreement, *supra* note 145, § 1.12.
[148] *Id.* § 2.5.1.
[149] E-gold, *supra* note 15.
[150] *See* E-gold Account User Agreement, *supra* note 145, § 4.3.
[151] *See, e.g.*, http://www.asianagold.com/ (last visited Nov. 19, 2008).
[152] *See* OmniPay, About Us, *supra* note 137 ("OutExchange" service exchanges e-metal for National currency).
[153] *See* e-gold, *supra* note 15.
[154] *See generally id.* (referencing outside, independent exchange services which support the exchange of national currencies and e-gold).
[155] A "spend" is "the act of transferring value between gold accounts in fulfillment of a payment order entered by User." E-gold Account User Agreement, *supra* note 145, § 1.12. A spend is based on the weight of e-gold and title is conveyed for the specific fine weight of metal, and is limited to the available balance. *Id.*
[156] *See* e-gold, *supra* note 15.

account of another currency exchanger that accepts e-gold in order to receive funds in a national currency.[157]

[42] Under the criminal charges against e-gold, the government alleged that e-gold, Ltd., Gold & Silver Reserve, Inc., and OmniPay together offered a payment processing service that constituted a money transmitting business in violation of 18 U.S.C. § 1960.[158] The indictment alleged that Gold & Silver Reserve, Inc. maintained bank accounts that accepted and transmitted wire transfers totaling millions of dollars, for the purpose of providing a digital currency exchange service.[159] It also alleged that OmniPay collected exchange fees from customers, in return for issuing quantities of e-gold.[160]

[43] E-gold and its co-defendants made several arguments in defense, contending that their operation did not consist of a "money transmitting business" as defined by 18 U.S.C. § 1960.[161] First, the e-gold defendants argued that to be a "money transmitting business," they must have engaged in cash transactions.[162] Since they did not accept hard currency or cash, they could not be a "money transmitting business."[163]

[44] A violation of the federal registration requirement under 18 U.S.C. § 1960(b)(1)(B) requires failure to "comply with the money transmitting business registration requirements under Section 5330 of Title 31 of the United States Code, or regulations prescribed under such section."[164] Thus, the e-gold defendants turned to the registration requirements of 31 U.S.C. § 5330, requiring a "money transmitting business" to register with the U.S. Treasury Department.[165] The definition of "money transmitting business" contains three subsections: (A), (B), and (C), which are listed in

[157] *See id.*
[158] E-gold Indictment, *supra* note 19, at 19.
[159] *Id.* at 22.
[160] *Id.* at 20.
[161] Memorandum of Law in Support of Defendants' Motion to Dismiss, *supra* note 21, at 5-9.
[162] *See id.* at 5-7.
[163] *See id.* at 8-9.
[164] 18 U.S.C. § 1960(b)(1)(B) (2006).
[165] *See* Memorandum of Law in Support of Defendants' Motion to Dismiss, *supra* note 21, at 5.

the conjunctive.[166] Subsection (B) mentions that the business must be required to file reports under 31 U.S.C. § 5313.[167] This statute, in turn, requires the filing of reports for transactions involving U.S. coins or currency.[168] Therefore, the e-gold defendants argued that a business is only a "money transmitting business" when it engages in transactions of coins or currency and is consequently subject to the reporting requirements of 31 U.S.C. § 5313.[169]

[45] Alternatively, the e-gold defendants argued that the criminal statute was unconstitutionally vague.[170] Although the statute requires that a defendant be subject to reporting under 31 U.S.C. § 5313, which requires a defendant to engage in currency transactions, 18 U.S.C. § 1960 defines "money transmitting" differently. "Money transmitting," according to the definition in 18 U.S.C. § 1960, includes transfers by wire, check, draft, fax, or courier.[171] Because of the ambiguity of whether the definition of "money transmitting" in 18 U.S.C. § 1960 controls over the definition of "money transmitting business" in 31 U.S.C. § 5330, the statute is unconstitutionally vague.[172]

[46] These arguments were unlikely to succeed if the prosecution had progressed to trial. The statute, on its face, seems to reach conduct that includes facilitating transfers involving not only cash but other transfers as well. It defines a "money transmitter" to include transfers of funds "on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier."[173] The government took the position that because of this definition, the statute makes clear that it includes conduct beyond

[166] 31 U.S.C. § 5330(d)(1)(A)-(C) (2006).
[167] *Id.* § 5330(d)(1)(B).
[168] *Id.* § 5313(a).
[169] *See* Memorandum of Law in Support of Defendants' Motion to Dismiss, *supra* note 21, at 8.
[170] *See id.* at 9-11.
[171] 18 U.S.C. § 1960(b)(2) (2006).
[172] Memorandum of Law in Support of Defendants' Motion to Dismiss, *supra* note 21, at 10-11.
[173] *See* 18 U.S.C. § 1960(b)(2).

cash transactions.[174] It contended that the statute, on its face, is clear on the conduct proscribed and that it would be improper to import the meaning in 31 U.S.C. § 5330.[175] This argument makes more sense, as Congress would not have included the broad types of transfers listed in 18 U.S.C. § 1960(b)(2) if it intended the offense to be limited to the definition in 31 U.S.C. § 5330.

[47] The strongest argument against the e-gold defendant's position is that 18 U.S.C. § 1960 does not limit the offense to failure to comply with the registration requirements of solely the statute, 31 U.S.C. § 5330. Violations may also include failure to register as required by "the regulations prescribed under such section."[176] This inclusion effectively torpedoes the e-gold defendants' argument that a "money transmitting business" must engage in cash transactions. The regulations implementing 31 U.S.C. § 5330 clearly require registration of businesses that engage in all types of funds transfers, not just those transacting in cash.[177] The regulations specifically state that "money services businesses" must register with the Department of the Treasury.[178] "Money services businesses" are defined in 31 C.F.R. § 103.11(uu) to include:

> (5) Money transmitter –
> (i) In general. Money transmitter:
> (A) Any person, whether or not licensed or required to be licensed, who engages as a business in accepting currency, or funds denominated in currency, and transmits the currency or funds, or the value of the currency or funds, by any means . . . ; or
> (B) Any other person engaged as a business in the transfer of funds.[179]

[174] Government's Response to Defendants' Motion to Dismiss Counts Two, Three and Four of the Indictment at 5-9, United States v. E-gold, Ltd., 550 F. Supp. 2d 82 (D.D.C. Mar. 7, 2008) (No. 07-109).
[175] *See id.* at 6-8.
[176] 18 U.S.C. § 1960(b)(1)(B).
[177] *See* 31 C.F.R. § 103.11(uu) (2008).
[178] *Id.* § 103.41(a)(1).
[179] *Id.* § 103.11(uu)(5).

[48] The e-gold operation likely satisfies 31 C.F.R. § 103.11(uu)(5)(i)(A), as OmniPay accepted "funds denominated in currency" through wire and bank transfers in order to fund customers' e-gold accounts, and exchanged out e-gold currency through such electronic transfers. Even if the e-gold operation does not satisfy subsection 31 C.F.R. § 103.11(uu)(5)(i)(A), it almost certainly satisfies the broader subsection 31 C.F.R. § 103.11(uu)(5)(i)(B), which includes "any other person engaged as a business in the transfer of funds."[180] In either case, if the e-gold operation falls within the definition of a "money services business," the regulations require that it register.[181] It is difficult to conclude that the failure to register under the regulations does not subject it to liability under 18 U.S.C. § 1960.

[49] Interestingly, the e-gold defendants never argued that they were not a "money services business" under the regulations. Instead, they strategically chose to stay away from any discussion of the regulations, relying entirely on the argument that the elements of "unlicensed" and "money transmitting business" must be separate, and that defining "money transmitting business" must be uniform throughout the statute without regard to the three "unlicensed" prongs under Section 1960(b)(1).[182] The

[180] *Id.* § 103.11(uu)(5)(i)(A)-(B).
[181] *See id.* § 103.41(a)(1).
[182] Defendants' Reply to the Government's Opposition to Defendants' Motion to Dismiss Counts Two, Three and Four of the Indictment at 5-6, United States v. E-gold, Ltd., et al., 550 F. Supp. 2d 82 (D.D.C. Mar. 19, 2008) (No. 07-109). The statute reads:

> (b) As used in this section—
>
> (1) the term "unlicensed money transmitting business" means *a money transmitting business* which affects interstate or foreign commerce in any manner or degree *and*—
>
> (A) is operated without an appropriate money transmitting license in a State where such operation is punishable as a misdemeanor or a felony under State law, whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable;
>
> (B) fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section; or
>
> (C) otherwise involves the transportation or transmission of funds that are known to the defendant

defendants argue in the alternative regarding the definition of "money transmitting business": it is *either* the case that the appropriate definition of "money transmitting business" is the one provided by 31 U.S.C. § 5330 (including a requirement that the business engage in cash transactions), *or* that this criminal statute is so vague as to void it in its entirety.[183]

B. IMPLICATIONS OF THE E-GOLD CASE FOR FUTURE PROSECUTIONS

[50] E-gold's indictment and prosecution helped frame the bounds of the U.S. regulatory regime of digital currency providers and digital currency exchangers. The e-gold case was unique in several ways. First, the same entity combined the roles of digital currency provider and currency exchanger. Gold & Silver Reserve was essentially in control of both OmniPay and e-gold, Ltd., although e-gold, Ltd. operated with some independence.[184] Second, these entities and the founders were all subject to U.S. jurisdiction.[185] E-gold, Ltd., although incorporated in Nevis, apparently had records and files located at codefendant Dr. Jackson's home in Melbourne, Florida.[186] In addition, the e-gold website states that Gold & Silver Reserve serves as the "operator" of the e-gold system.[187] With Gold & Silver Reserve as a Delaware corporation headquartered in the United States, this would bring at least some of e-gold, Ltd.'s operations within U.S. jurisdiction. Third, the government included the charge of conspiracy in violation of 18 U.S.C. § 371, bringing the roles of

---

> to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity.

18 U.S.C. § 1960(b) (2006) (highlighting the E-gold defendants' argument that the "money transmitting business" prong must be decided independently of the "unlicensed" prong) (emphasis added).

[183] Memorandum of Law in Support of Defendants' Motion to Dismiss, *supra* note 21, at 1, 6-11.

[184] E-gold Indictment, *supra* note 19, at 6.

[185] *See id.* at 18-25.

[186] Meek, *supra* note 41.

[187] E-gold, Corporate History, http://www.e-gold.com/unsecure/aboutusdetail.html (last visited Nov. 19, 2008).

the digital currency provider, currency exchanger, and administration of each, under one criminal enterprise.[188]

[51] Conspiracy seemed to be a key component in the government's case against the founders. If each codefendant had a role independent of the other, and the digital currency provider in e-gold, Ltd. was in fact distinct from Gold & Silver Reserve, perhaps there could be no complete "business" as required by the statute. The statute's language, however, may still allow prosecution of the offense even where an entity does not constitute the entire "business." The first clause in 18 U.S.C. § 1960 includes the language, "[w]hoever knowingly conducts, controls, manages, supervises, directs, or owns all *or part* of an unlicensed money transmitting business."[189] This indicates that even an individual or entity that conducts and has knowledge of only part of the "money transmitting business" could be prosecuted under the statute. It is not yet clear how far this will extend, but the potential liability is broad. For example, is the e-gold employee in charge of managing its information technology department (as small or large as it may be) also liable for managing part of an unlicensed transmitting business? The few courts considering the issue have held that the offense is a general intent crime, requiring only that the defendant have knowledge as to the conduct of the factual elements, not knowledge of the reporting requirements or the offense.[190] Construed broadly, this means that those who direct, manage, or supervise only part of an operation that later, combined with another entity, becomes a money transmitting business, may be subject to criminal liability under 18 U.S.C. § 1960.

[52] As for the e-gold prosecution, the government's theory was that e-gold, Ltd., OmniPay, and Gold & Silver Reserve conspired to form a jointly run "money transmitting business."[191] The defendants may have attempted to insulate themselves by separating the digital currency provider, e-gold, Ltd., from the rest of the operation. If they could sufficiently separate the digital currency provider from the exchanger, they

[188] E-gold Indictment, *supra* note 19, at 18-25.
[189] 18 U.S.C. § 1960(a) (2006) (emphasis added).
[190] United States v. Talebnejad, 460 F.3d 563, 572 (4th Cir. 2006); United States v. Keleta, 441 F. Supp. 2d 1, 2 (D.D.C. 2006); United States v. Uddin, 365 F. Supp. 2d 825, 829 (E.D. Mich. 2005).
[191] E-gold Indictment, *supra* note 19, at 18-19.

could argue either that the operation as a whole did not constitute a "business" as required by the statute, or that they did not have knowledge that one piece or the other was unlicensed. The problem for the defendants is that Gold & Silver Reserve still operated parts of the e-gold currency transactional operations, and, therefore, the separation was incomplete.[192]

[53] Because of this problem, it was more difficult for the defendants to make the argument that e-gold, Ltd. did not know that Gold & Silver Reserve was unlicensed, or vice versa. In addition, the government brought forward an alternative theory in the indictment.[193] It alleged that the e-gold operation "did not require other individuals or entities offering 'e-gold' exchange services to be licensed or registered as a money transmitting business, nor did it concern itself with the policies and practices of those exchangers related to the acceptance of cash or other funds, or the true identification of the exchangers' customers."[194] If the e-gold operation knew that the exchangers with whom it dealt were unlicensed, then this may fulfill the general intent requirement of "knowingly" conducting "part of an unlicensed money transmitting business."[195] The government would still have to prove that e-gold had knowledge that its services satisfied the factual elements of a "money transmitting business." Even if e-gold, Ltd. itself were not required to register, a showing that it knew the exchangers were themselves unlicensed may satisfy this element.

[54] There is some evidence in the regulations to suggest that a digital currency provider, particularly one tied to a commodity such as a precious metal, may fall under exceptions to the registration, reporting, and recording requirements.[196] The catch-all provision of the regulations, which subjects a person or entity to the registration requirement, and defines "money transmitter" as "any other person engaged as a business in the transfer of funds," is limited by the "facts and circumstances" of each case.[197] The regulations state that "the acceptance and transmission of

[192] *Id.* at 6, 21-22.
[193] *Id.* at 20-21.
[194] *Id.* at 21.
[195] 18 U.S.C. § 1960(a) (2006).
[196] *See* 31 C.F.R. § 103.11(uu)(5)(ii) (2008).
[197] *Id.*

funds as an integral part of the execution and settlement of a transaction other than the funds transmission itself . . . will not cause a person to be a money transmitter."[198] This could be interpreted to mean that an entity operating only as a commodity exchange mechanism, transmitting funds only for the purposes of settling accounts, is not a "money transmitter" and thus not subject to the registration requirement.[199]

[55] Thus, it might be possible for one to maintain a digital currency provider independently, without offering exchange services, without being subject to the regulations. If the digital currency provider itself is not "engaged in the business" of transmitting funds as defined in the regulations, it would not be subject to criminal liability under 18 U.S.C. § 1960.[200] For example, e-gold, Ltd. itself would have an argument that since it only charges enough to maintain storage of the gold bullion, it is not actually in the "business" of transmitting funds.[201] Alternatively, it is unclear that liability would ensue for e-gold, Ltd. if the currency provider was entirely outside United States jurisdiction, and therefore not subject to reporting requirements. Successful prosecution in such a case would have to prove that e-gold, Ltd. knew that the foreign entity was "engaged in the business" of transmitting funds.[202] Also in question in such a case would be the knowledge of the "unlicensed" element.[203] If the foreign digital currency exchanger is not subject to the United States' jurisdiction, then it has no obligation to be licensed under law. The question becomes whether it would be enough for the government to prove that the digital currency provider had knowledge of the factual elements that are required for an entity to be considered a "money transmitting business," and that its own part of this overall business was unlicensed.[204] Perhaps it could be a defense that a digital currency provider subject to United States jurisdiction reasonably believed that the exchangers with whom it was doing business fulfilled legal registration requirements in their own jurisdictions.

---

[198] *Id.*
[199] *See* Hughes et al., *supra* note 90.
[200] *See* 18 U.S.C. § 1960(a).
[201] E-gold, *supra* note 15 (using Agio fee to recover bullion storage costs).
[202] 18 U.S.C. § 1960(a).
[203] *See id.* § 1960(a)-(b).
[204] *See id.*

[56] As United States regulations become more stringent and prosecutions more prevalent for digital currency providers and exchangers, it is inevitable that these entities will move, in whole or in part, to locations abroad with less regulation.[205] In this process, several questions arise regarding the United States' ability to protect against the transmission of funds in support of criminal activity: To what extent are digital currency providers and exchangers subject to United States jurisdiction if they are located outside the United States, but have individuals within the United States using their services online? In addition, what kind of international regulations and agreements exist to address these new methods of transmitting funds? The next section examines the international nature of these entities and how they challenge jurisdictional limitations of financial regulations.

IV. INTERNATIONAL AGREEMENTS AND INTERNATIONAL REGULATION OF FINANCIAL INSTITUTIONS

[57] An international focus on financial regulation, specifically on terrorist finance, has begun only recently.[206] The International Convention for the Suppression of the Financing of Terrorism, signed in 2000, made it an offense to provide or collect funds with the knowledge that they would be used to finance terrorist acts.[207] The Convention also imposed "know your customer" and suspicious activities reporting requirements,[208] and has been ratified by 150 countries.[209]

[58] The Financial Action Task Force (FATF), created at the G7 Paris summit in 1989, has been one of the most active international groups in discussing and implementing measures designed to inhibit terrorist

[205] *Cf.* U.S. DEPT. OF TREASURY, 2007 NATIONAL MONEY LAUNDERING STRATEGY vi (2007), *available at* http://www.treas.gov/press/releases/docs/nmls.pdf ("[a]s it becomes more difficult to move illicit funds . . . there is a clear migration to other channels.").
[206] Donohue, *supra* note 4, at 381.
[207] International Convention for the Suppression of the Financing of Terrorism art. 2, *adopted* Dec. 9, 1999, 2178 U.N.T.S. 197.
[208] *Id.* art. 18.
[209] OFFICE OF THE COORDINATOR FOR COUNTERTERRORISM, U.S. DEPT. OF STATE, COUNTRY REPORTS ON TERRORISM: INTERNATIONAL CONVENTIONS AND PROTOCOLS ON TERRORISM (2007), *available at* http://www.state.gov/s/ct/rls/crt/2006/83238.htm.

financing.[210] FATF was originally designed to serve as a tool to combat international money laundering.[211] Its mandate was later expanded to include creating standards to fight the financing of terrorism. In 1990, FATF issued forty recommendations to combat money laundering, with updates occurring in 1996 and again in 2003.[212] One result was the creation of the Non-Cooperative Countries and Territories List (NCCT), which identifies those countries that fail to meet the regulations advanced by FATF.[213] The forty recommendations involve increased customer due diligence and recordkeeping, and reporting of suspicious transactions.[214] Additionally, FATF issued nine special recommendations to combat the financing of terrorism, expand suspicious activities reporting, and require the licensing of alternative remittance systems or any entity that provides a service of transmitting funds or value.[215] Although neither the forty recommendations nor the subsequent nine recommendations directly address digital currencies, in 2006, FATF conducted a study and issued a report on new payment systems, including different forms of digital currencies.[216]

[59] While none of the FATF recommendations are binding, the creation of the NCCT has been effective in pressuring countries to impose more stringent financial regulations. For example, the initiative began listing countries as non-cooperative in 2000. In reviewing 47 countries, 23 were listed as non-cooperative.[217] As of October of 2006, no countries remained on the list, although the initiative continues to monitor

[210] FINANCIAL ACTION TASK FORCE, ABOUT THE FATF, http://www.fatf-gafi.org (follow "About the FATF" hyperlink) (last visited Nov. 19, 2008).
[211] *Id.*
[212] FINANCIAL ACTION TASK FORCE, The 40 Recommendations, (2003), http://www.fatf-gafi.org (follow "40 Recommendations" hyperlink).
[213] FINANCIAL ACTION TASK FORCE, About the Non-Cooperative Countries and Territories (NCCT) Initiative, http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236992_1_1_1_1_1,00.html (last visited Nov. 19, 2008).
[214] FINANCIAL ACTION TASK FORCE, The 40 Recommendations, *supra* note 212.
[215] FINANCIAL ACTION TASK FORCE, 9 Special Recommendations (SR) on Terrorist Financing (TF), (2004), http://www.fatf-gafi.org (follow "9 Special Recommendations" hyperlink).
[216] *See* FATF REPORT ON NEW PAYMENT METHODS, *supra* note 27, at 1.
[217] FATF, About the Non-Cooperative Countries and Territories (NCCT) Initiative, *supra* note 213.

progress.[218] Despite these efforts and successes in persuading countries to enact stricter regulations, the porous nature of the Internet and electronic communications still presents enormous challenges to combating the financing of terrorism. The Internet, by its own nature, defies regulations that are confined to a geographic nation-state; individuals can access websites from anywhere in the world, thereby making effective regulation difficult.[219]

[60] As the United States continues to transition from legislation and regulations designed to combat money laundering to a regime that also effectively combats terrorist financing, there are two main areas of focus. First, the United States must examine its regulations of digital currency providers and currency exchangers that are located in the United States, or subject to its jurisdiction. Second, it must focus on what it can do to prevent the use of digital currency providers located abroad to transfer funds that can be accessed and spent within the U.S. to carry out terrorist operations. The following section discusses current U.S. regulations of digital currency providers and exchangers, offering suggestions to bolster this regime and lower the risks posed by digital currency transactions. Part VI follows with a discussion on what the U.S. can do to mitigate the risks posed by those digital currency providers and exchangers located outside its jurisdiction.

V. POLICY RECOMMENDATIONS TO LOWER THE RISKS OF DIGITAL CURRENCIES

A. MEASURES TO LOWER THE RISK OF DOMESTIC CURRENCY PROVIDERS/EXCHANGERS

[61] In order to implement sufficient domestic financial regulations it is useful to analyze the risk posed by digital currencies by analogizing to cash transactions.[220] Those engaged in illegal activity prefer to use cash when possible because it is "anonymous, untraceable, requires no intermediary, is widely accepted, and provides for immediate

[218] FATF, Non-Cooperative Countries and Territories, http://www.fatf-gafi.org/document/4/0,3343,en_32250379_32236992_33916420_1_1_1_1,00.html.
[219] *See* MONEY LAUNDERING IN DIGITAL CURRENCIES, *supra* note 28, at 1.
[220] *See supra* Part I.B.

settlement."[221] In a 2006 report, FATF identified characteristics of digital currencies that increase the risk that such currencies will be used to finance terror operations.[222] Digital currencies pose a higher risk where they (1) afford a higher level of anonymity; (2) have no limit on the transaction size; (3) leave no traceable record; (4) have a wide range of funding methods; (5) have no geographical limit; and (6) have no limit to what they may purchase, or no limit on their transferability to hard cash.[223] Regulations should be aimed at reducing or eliminating each of these risks.[224]

[62] First, the regulations should specifically apply to digital currency providers. As discussed above in Part III.B., a digital currency provider that does not offer exchange services currently may fall under an exception to the regulations and escape registration, record-keeping, and reporting requirements.[225] Under the definition of "money transmitter" in 31 C.F.R. § 103.11(uu), the regulations suggest that acceptance and transmission of funds to settle an account, in connection with the sale of a commodity or other instrument of value, alone will not cause one to be a "money transmitter."[226] To eliminate this possible loophole for digital currency providers, the regulations should specifically include them in the definition of a "money transmitter." This could be accomplished by broadly defining "money transmitter" to include, for example, "any person engaged in maintaining an online funds transfer system." If the Treasury Department desired to exempt certain businesses, such as those connected with securities or other property, it could specifically list these types of businesses as exempt. In addition, retaining the language, "engages in the business" for this category provides another loophole for companies like e-gold, Ltd., which claims it does not operate for profit, but merely charges a small exchange fee for the purposes of covering the bullion storage costs. Eliminating the "engages in the business" requirement from the digital currency provider category would ensure coverage of these entities.

---

[221] FATF REPORT ON NEW PAYMENT METHODS, *supra* note 27, at 10 n. 22.
[222] *Id.* at 10-11 tbl.2.
[223] *Id.* at 10-11.
[224] See *id.* at 18 for a list of current and potential risk mitigants.
[225] *See supra* Part III.B.
[226] 31 C.F.R. § 103.11(uu)(5)(B)(ii) (2008).

[63] After making all digital currency providers subject to the regulations, one can consider whether the current identification and verification requirements are sufficient for the "money services business" category. Currently, "money services businesses" must implement minimum procedures for verifying the identities of all customers.[227] The regulations provide more specific guidelines for transactions of $3,000 or more.[228] Non-bank financial institutions must record the name and address of the transmitter, the date and amount of the transfer, identity of the recipient's institution, and the recipient's name, address, account number, and taxpayer number (such as social security number, or passport number).[229] Although the regulations outline strict recording requirements for transactions of $3,000 or more,[230] they are vague as to the customer verification required for lesser transactions.[231] It would be better to specifically define what information is required for all customers, such as providing name, address, and phone number, and requiring the money services business to verify the information by contacting the customer through one of these means. Regulations should also require money services businesses to maintain records of the information in addition to verifying it, to ensure its availability for possible investigations.

[64] Customers are currently limited as to the amounts transferred from one U.S. digital currency account to another based on the information they must furnish for transactions of $3,000 or more.[232] Regulations could further lower the risk posed by digital currency transactions by placing limits on the methods used to convert the digital currencies to cash, such as on the issuance of cash cards by currency exchangers, or on wire transfers cashing out digital currency accounts. Use of a check or wire transfer would route the transaction through a bank, and thus, trigger the regulations required of banks.[233] The use of a cash card, however, would not, as the entity in charge of issuing the card is responsible for setting the

[227] *Id.* § 103.125(d)(1)(i)(A).
[228] *Id.* § 103.33(f).
[229] *See id.* § 103.33(f)(2) (requirements for those "other than established customers"); *see id.* § 103.11(l) (requirements for "established customers").
[230] *See id.* § 103.33(f).
[231] *Id.* § 103.125(d)(1)(i)(A) (2008).
[232] *See id.* § 103.33(f)(1).
[233] *See id.* § 103.33(e).

limits to its use.[234] For any exchange using a cash card, regulations should require the recording of the same information as for transactions of $3,000 or more, making it more difficult for individuals to remain anonymous.

[65] Another possibility would be to place a value limit on cash cards, and per day and per year limits on spending, as well limits on the number of such cards an individual may purchase. For example, the EU has implemented regulations exempting issuers of cash cards from due diligence requirements, as long as those cards abide by certain value limitations.[235] A card issuer need not take measures to identify customers purchasing non-rechargeable cards of 150 Euros or less, or rechargeable cards with a yearly charging limit of 2,500 Euros and a yearly spending limit of 1,000 Euros.[236]

[66] Europe's limits on cash cards do not consider the source of the electronic money loaded on the card.[237] The threshold limits, below which the issuer is exempt from due diligence requirements, seem to be designed more for gift card applications. For example, a store that issues such cards, redeemable only at its own stores, would not want to be burdened with collecting identifying information for each card sold. The risk of illegal use is also lower for these limited-use cards.[238] Unfortunately, Europe's exemption would also apply to cash cards issued by a currency exchanger that redeems digital currencies. These cards are higher risk because they can be loaded online and redeemed at any ATM.[239] Thus, they should be subject to more stringent regulations and they should not be exempt from due diligence requirements.

[67] The goal of regulating digital currency providers and exchangers is to set limits that allow customers the freedom to utilize new, innovative methods of transferring funds, while at the same time lowering the risk that such methods may be used to finance terror operations or other illegal

[234] *See, e.g.*, Visa Reloadable Prepaid Card: FAQ, http://usa.visa.com/personal/cards/prepaid/reloadable_prepaid_card_faq.html#anchor_12 (last visited Nov. 19, 2008).
[235] Council Directive 2005/60, arts. 7, 8, 11(5)(d), 2005 O.J. (L 309) 15, 23-25 (EC).
[236] *Id.* art. 11(5)(d), at 24-25.
[237] *See id.* at 25.
[238] FATF REPORT ON NEW PAYMENT METHODS, *supra* note 27, at 4, 13.
[239] *See id.* at 11-12.

activities.[240] The United States should consider placing further limits on cash cards issued by currency exchangers that accept digital currencies. These entities should not be exempt from the due diligence requirements entirely, as most transactions will likely occur online instead of in person. A graduated system would best maintain the balance between customer freedom and management of risk. As the amount of value on the card increases, the recording and due diligence requirements should also increase. Purchases of cards with values of $3,000 or higher should be subject to a higher standard of customer identification and recordkeeping. This would be consistent with the current regulations for other financial institutions, which require additional measures for transactions of $3,000 or more.[241]

B. MEASURES TO LOWER THE RISKS ASSOCIATED WITH INTERNATIONAL DIGITAL CURRENCY PROVIDERS AND EXCHANGERS

[68] With increased regulation in the United States and increased enforcement through prosecutions like the e-gold case, digital currency providers and exchangers have an incentive to move to locations abroad with more favorable laws.[242] Although FATF has worked toward pressuring countries to enact minimum financial regulations, there are still jurisdictions which have fewer regulations and less stringent enforcement.[243] International efforts remain important to eliminate loopholes that may allow digital currency providers to operate in an under-regulated environment.

[69] As already mentioned, financial regulations have the dual purpose of preventing illegal money flows and creating a paper trail for later investigations.[244] It will likely be impossible to detect and prevent all transfers of funds intended to support terror attacks in the United States without placing a significant burden on the financial sector and on

[240] *See supra* Part II.A.
[241] *See* 31 C.F.R. § 103.33(f) (2008).
[242] *See supra* note 205 and accompanying text.
[243] *See FATF Statement on Certain AML/CFT Deficiencies*, FATF E-NEWS, Mar. 2008, at 2, *available at* http://www.fatf-gafi.org/dataoecd/42/37/40305148.pdf; *see also* FATF REPORT ON NEW PAYMENT METHODS, *supra* note 27, at 17 (discussing the differences of laws and regulations within the jurisdictions).
[244] *See supra* Part II.A.

innocent citizens who transfer funds every day. It is equally important, however, that a paper trail exist so that investigators can later use records in conjunction with other evidence to vet potential suspects more quickly. The recording requirements and customer verification information could be vital to efforts to locate an individual before an attack occurs.

[70] The greatest threat that digital currency providers and exchangers outside U.S. jurisdiction pose is an anonymous avenue for individuals to acquire usable funds within the United States. Digital currency providers such as e-gold pose a greater threat when they move abroad where they are able to avoid the U.S. regulatory regime. Individuals can access the Internet from anywhere in the world, transfer funds via a digital currency, and convert the account into usable funds through a cash card service. This mechanism of transferring funds into the U.S. would thwart the current U.S. financial checks that are meant to detect and prevent, or at least document, questionable transfers that might be used to finance terror operations. An individual could visit several different ATMs using one or more cash cards, withdraw the maximum amount allowed, and within a short time period extract several thousand dollars worth of cash without having any personal information recorded and without leaving a paper trail in the United States.

[71] The United States could better protect itself against such transfers in several ways. First, as the EU has done, the United States could place limits on the issuance of prepaid cash cards by U.S. financial institutions, including maximum loading limits, per day and per year spending limits, and limits on the number of cards that an individual may purchase.[245] If the issuance of a cash card exceeded the limits, it would be subject to due diligence, recording, and reporting requirements. Second, the U.S. could prohibit U.S. financial institutions from issuing prepaid ATM/debit cards for international currency exchangers dealing in digital currencies that are not subject to U.S. regulations. This measure would be more difficult to enforce, however, and would likely require a U.S. regulatory agency to identify and publish the names of blacklisted foreign issuers of cash cards.

[72] Third, the U.S. could prohibit financial institutions that operate ATMs and merchant banks in the U.S. from honoring transaction requests

[245] *See supra* notes 234-237 and accompanying text.

from international currency exchangers and banks that have issued prepaid ATM/debit cards in exchange for digital currencies. This proposal is more complex and requires a brief discussion of how debit and ATM transactions function. An ATM/debit card (or cash card) transaction generally involves three players: an issuing bank or entity (business abroad issuing the cash card), a cardholder, and the acquiring bank (bank in the United States operating the ATM).[246] This discussion focuses on those transactions where the cardholder uses a PIN, the most common way to extract physical cash from an account.[247] The focus of this article is on the danger presented by the anonymous transfer of funds from abroad to usable cash in the United States. In such a scenario, an individual in the U.S. inserts a cash card into an automated teller machine (ATM), requesting cash. The U.S. bank or institution operating the ATM sends an authorization request through a card system network (such as Maestro, Cirrus, or Star) to the issuing bank or institution.[248] When the issuing institution of the cash card grants authorization, the ATM dispenses the requested cash, and settlement between the banks or institutions may occur immediately or at a later time.[249] The individual receives the cash anonymously, without customer information being verified or recorded. The loophole occurs where the issuer of the card is outside the United States, beyond the regulatory regime's jurisdiction. Although both the institution operating the ATM and the card system network may be subject to U.S. jurisdiction, they have no information about the cardholder, and the only information recorded is the amount of withdrawal and the foreign issuing bank or institution.

[73] A solution to prevent such an anonymous transfer would be to require those entities subject to U.S. jurisdiction, the institution operating the ATM or the card system network, to either obtain and record sufficient

[246] BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM AND DEPARTMENTAL OFFICES, DEPARTMENT OF THE TREASURY, NOTICE OF JOINT PROPOSED RULEMAKING: PROHIBITION ON FUNDING OF UNLAWFUL INTERNET GAMBLING 9 (2007), *available at* http://www.treas.gov/press/releases/reports/noticeofproposedrule.pdf [hereinafter PROHIBITION ON FUNDING OF UNLAWFUL INTERNET GAMBLING].

[247] Debit card transactions may also be processed like a credit card, through payment networks such as Mastercard or Visa. Such a transaction would also include a fourth player, the merchant. *See id.*

[248] FATF REPORT ON NEW PAYMENT METHODS, *supra* note 27, at 26-27.

[249] PROHIBITION ON FUNDING OF UNLAWFUL INTERNET GAMBLING, *supra* note 246.

customer information in the authorization process, or to altogether deny requests for withdrawals from foreign currency exchangers that issue cash cards. One concern is that this approach might impose too large a burden on U.S. financial institutions to obtain such information or to keep track of foreign entities, for which they must refuse to honor transaction requests. Yet, the United States has already convinced many banks to voluntarily decline to process certain transactions in the Internet gambling context. [250] This indicates that it is possible for banks to selectively decline transactions from specific entities. In the case of online gambling, merchants are required to code customer purchases; this allows credit card companies to decline charges that reference gambling codes.[251] The concern is that merchants may cheat and code charges as something else, or route them through another merchant.[252] The most effective mechanism would be to prohibit honoring transactions altogether with foreign currency exchangers that accept digital currencies and issue cash cards. To enforce such a system, the U.S. Treasury Department, or other government agency, would have to maintain a list of such currency exchangers. Regulations would require U.S. banks operating ATMs to periodically update their systems to reflect blacklisted foreign entities. Although the precise mechanics and implementation of this potential solution are beyond the scope of this article, it is a solution that regulators and those in the banking industry should discuss. The goal of the above proposed measures is to protect against anonymous transfers of funds without overburdening consumers or the banking industry.

VI. CONCLUSION

[74] Digital currencies and exchangers dealing in such currencies present a risk to the United States and other nations if the applicable regulations remain ambiguous. Allowing users of digital currencies and prepaid cash

[250] Christine Hurt, *Regulating Public Morals and Private Markets: Online Securities Trading, Internet Gambling, and the Speculation Paradox*, 86 B.U. L. REV. 371, 435 (2006); Andrea L. Marconi & Brian M. McQuaid, *Betting And Buying: The Legality of Facilitating Financial Payments for Internet Gambling*, 124 BANKING L.J. 483, 496 (2007).

[251] I. NELSON ROSE & MARTIN D. OWENS, JR., INTERNET GAMING LAW: GAMBLING AND THE LAW 210 (2005).

[252] Gambling providers risk being blacklisted by credit card providers and associations when they change coding in an attempt to evade detection. *See id.*

cards to take advantage of these services without identification or customer verification requirements increases the risk of exploitation by money launderers and those seeking to finance terrorism. The first step will be to tighten U.S. regulations as they apply to digital currency providers and currency exchangers, especially those offering prepaid cash cards.

[75] The e-gold case highlights other potential legal issues surrounding the regulation of digital currencies. Specifically including digital currency providers in the "money services businesses" category would foreclose many of the arguments made by the e-gold defendants and others that such businesses are not subject to prosecution under the unlicensed money transmitting business offense. In addition, the "engages as a business" exception should not apply to digital currency providers, as long as the definition makes it clear that individual liability would ensue only for operating or maintaining a currency system, and not simply for using such a system. These measures to regulate domestic operators of digital currencies should be relatively uncontroversial and simple to implement.

[76] The greatest challenge of digital currencies is their tendency to transcend jurisdictional boundaries, making effective regulation difficult. International cooperation through organizations like FATF will be critical in addressing this and many other challenges. In addition, the United States should consider taking steps on its own to protect against the risks presented by digital currencies. These may include requiring banks that operate ATMs and accompanying card system networks to honor only prepaid cash cards issued by financial institutions licensed in the United States and dishonor transaction requests from unlicensed institutions.

[77] Successfully protecting against the risks posed by digital currencies and other new payment methods will require ideas from regulators, domestic financial institutions, foreign countries and entities, and international organizations. The risks of digital currencies cannot be mitigated by domestic efforts alone. It is increasingly important to work within the framework of multilateral institutions, such as FATF, as newer technologies and fund-transfer methods evolve. The goal of regulating these new technologies should be to mitigate the risks posed by potential criminal uses without completely stripping consumers of the legitimate benefits that these technologies offer. Digital currencies provide

consumers with an additional method of exchange, but left unchecked, such currencies have the potential to be exploited by money launderers and financiers of terrorism. Regulators should increase their awareness of digital currencies and work together with the banking industry and international partners to address the risks posed by these new fund-transfer methods.