NOTE

PROGRESS, PRIVACY, AND PREEMPTION: A STUDY OF THE REGULATORY HISTORY OF STORED-VALUE CARDS IN THE UNITED STATES AND THE EUROPEAN UNION

Naomi Claxton*

I. BACKGROUND AND INTRODUCTION

Over the last decade, prepaid stored value cards (SVCs) have begun to enjoy a position of relevant prominence in the global financial market. From phone cards to gift cards, the market for "unbanked" consumers has rapidly proliferated and includes both one-time use and reloadable SVCs that can be loaded with amounts up to, in some cases, $10,000 at a time.[1] Although the first SVCs were phone cards promulgated in Italy,[2] Europe has largely been left behind in the growth of the market for stored value cards.[3] In the United States, however, the current market in prepaid SVCs includes gift cards, travel cards, payroll cards, and so-called "teen cards," which allow those under 18 to access funds that their parents load onto the cards, flexible spending account cards, employee incentive cards, and subway cards.[4] The United States eagerly embraced the realm of gift cards while the European Union approached the emergence of the gift card market with regulations and limitations that have worked to effectively limit the availability of stored value cards to European consumers.[5] During the 2007 holiday season, for instance, U.S. consumers spent $26.3 billion dollars on gift cards in stark contrast to the European Union, which was projected to reach a mere $2.3 billion in annual consumption by 2010.[6] A major reason that Europe has not

---

* J.D. Candidate, 2011, University of Arizona James E. Rogers College of Law.

1. *See generally* Ethan Zindler, *Prepaid Cards Give Rise to Laundering Concerns*, AMERICAN BANKER, Nov. 7, 2005 at 1.

2. *History of Prepaid Cards*, LDPOST, http://www.ldpost.com/telecom-articles/The-History-of-Prepaid-Phone-Cards.html (last visited Dec. 31, 2011).

3. *Id.*

4. Mark Furletti, *Prepaid Card Markets & Regulation* (Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper No. 04-01, Feb. 1, 2004), *available* at http://www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/2004/Prepaid_022004.pdf; George Blum, *Regulation of Pre-Paid Stored-Value "Gift Cards,"* 46 A.L.R. 6TH 437, § 2 (2009); Christopher Woods, *Stored Value Cards*, 59 CONSUMER FIN. L. Q. REP. 211 (2005).

5. Malte Krueger, *E-Money Regulation in the EU*, *in* E-MONEY AND PAYMENT SYSTEMS REVIEW 239-251 (Robery Pringle & Matthew Robinson eds., 2002).

6. *MasterCard Launches a Guide to Prepaid Cards for Consumers*, INSIDEMONEYTALK (Apr. 19, 2007), http://www.insidemoneytalk.com/news/mas/mas104.html; Rich Mitchell, *Gift Cards Are Just the Start*, *available at* http://www.docstoc.com/docs/27162070/Gift-Cards-Are-Just-the-Start (last visited Dec. 31, 2011).

embraced the SVC trend is due to concerns about fraud at the point of sale.[7] In the United States, the transactions are sent directly to the bank and, for the most part, the issuing bank always knows how much value is left on the card and the balance cannot be "overdrawn."[8] In Europe, not all transactions are processed online, so there are concerns that people would be able to spend more than they had loaded onto the card.[9]

This Note compares the regulatory regimes of the United States and the European Union, and urges that consistent and comprehensive regulation of issuers and consumers of SVCs—though less intensive than that enacted in the European Union—is necessary to curb money laundering and staunch the flow of illegal fund transfers into and out of the United States. Because of the European Union's proactive legislation regulating the use of SVCs, it is likely that it will experience a much lower level threat from money laundering, will see lower instances of criminal fund transfers, will regulate suspicious activity more successfully, and will have greater success identifying those who engage in money laundering activities. In the United States, however, 18 U.S.C. § 1960 and Title III of the Patriot Act are, or may be, far more effective tools for effective criminal prosecution of money launderers and civil prosecution for banks and non-bank financial institutions (NBFIs) that violate a more stringent set of proposed regulations designed to create an environment where, at least for open and semi-open system gift cards, the seller is completely known to the buyer.[10] This Note also explores the regulatory convergence: the United States has begun to regulate SVCs more stringently in the post-911 era, and the European Union has begun a gradual relaxation of its stringent legislation. Finally, this Note compares the approaches to SVC regulation and anti-money laundering that have been taken in Germany and Arizona as systems that have experienced and dealt with criminal prosecutions for money laundering.

A. Recent Money Laundering Prosecutions

The indictment of the SVC "company" Moola Zoola in the U.S. District Court of Texas is a useful example of how criminals involved in money laundering can prey on the SVC industry. In 2007, entrepreneur Robert Arbuckle, president and CEO of prepaid debit card company Moola Zoola, was arrested for conspiracy

7. *See* European Central Bank, *Issues Arising From the Emergence of Electronic Money*, ECB MONTHLY BULLETIN, Nov. 2000, *available at* http://www.ecb.int/pub/pdf/other/pp49_60_mb200011en.pdf [hereinafter ECB].

8. *See* Furletti, *supra* note 4.

9. ECB, *supra* note 7.

10. 31 U.S.C.A. §§ 5311-30 (West 2003 & Supp. 2007); 12 U.S.C.A. §§ 1818(s), 1829(b), 1951-59 (West 2000 & Supp. 2007); *see* Patriot Act, Pub. L. No. 107-56, 115 Stat. 311 (2001) (codified in scattered sections of U.S.C.).

to commit fraud and launder money.[11] Arbuckle operated a scheme whereby he obtained money by defrauding consumers in Europe and North Carolina online using PayPal accounts to charge Moola Zoola cards.[12] These Moola Zoola cards were then used to charge other Moola Zoola cards, which were then used to withdraw cash from ATMs from Texas to Russia.[13] Moola Zoola was a distributor of both SVCs and ATM cards, but as a practical matter, its SVCs were the primary tool used to move the money around before the money was ultimately withdrawn on an ATM card.[14]

The Moola Zoola case represents a quite simplistic scheme in that it began with a scam that was likely reported early. The funds that were "laundered" were obtained through a PayPal scam by which individual PayPal accounts of customers in Europe and North Carolina were hacked and funds were transferred electronically directly onto a Moola Zoola card, then on to other Moola Zoola cards.[15] Because the victims were likely to report the initial transactions, it was a scheme that was guaranteed to—and did—get immediate attention; and, eventually, prosecution. Assistant U.S. Attorney Ernest Gonzalez was quoted as saying that the prepaid cards were "used to launder money all over the world."[16] Mr. Arbuckle's scheme was not particularly sophisticated in that it was not simply a scheme to launder money or move it undetected through the U.S. financial system. Instead, it originated with fraud and was therefore easy for prosecutors to "follow the ball," so to speak. In late 2006, Mr. Arbuckle was charged with 152 counts of identity theft for this activity, and his personal assets were seized.[17] In situations where the money is the legal possession of the transferor, however, the situation can be quite different.

Western Express International, Inc., a company involved in a much more complex and high profile prosecution involving SVCs, was set up as a domestic business corporation in Manhattan in 1997.[18] The company's main line of work was shipping, check cashing, and sale of digital currencies and gift cards.[19] In February 2006, Vadim Vassilenko, Yelena Barysheva, and Alexey Baryshev were indicted by the State of New York for operating an illegal money transmittal

11. Tiara M. Ellis, *Frisco Man Charged with Running ID Theft Ring*, DALLAS MORNING NEWS, Nov. 23, 2006, *available at* http://www.tmcnet.com/usubmit/2006/11/23/2109263.htm.

12. Ed Maldonado & Matthew Schullman, *Regulatory Rundown: The FCC Cracks Down*, PREPAID PRESS, Apr. 16, 2007, *available at* http://www.prepaid-press.com/news_detail.php?t=paper&id=1714.

13. *Id.*

14. *Id.*

15. Ellis, *supra* note 11.

16. Stanley Sienkiewicz, *Prepaid Cards: Vulnerable to Money Laundering?*, 12 ELEC. BANKING L. & COM. REP. 7 (2007).

17. Ellis, *supra* note 11.

18. Thomas Claburn, *Seventeen Indicted for Cybercrime and ID Theft in New York*, INFORMATIONWEEK (Nov. 09, 2007, 03:00 PM), http://www.informationweek.com/news/202804370.

19. Sienkiewicz, *supra* note 16.

business.[20] Western Express, Inc., their company, exchanged criminal proceeds for digital proceeds—including SVCs. On its websites, Western Express openly solicited customers in Eastern Europe, Russia, and the Ukraine, to operate illegally in the United States.[21] Western Express owners and operators solicited foreign business owners who were looking to conduct spamming, phishing, and identity theft in the United States but needed a "legitimate" online identity.[22] According to the indictment, Western Express owners and operators "promoted, facilitated, and aided in the purchase, sale and fraudulent use of stolen credit cards and other personal identifying information through various computer services."[23] Later, these identities were sold to the overseas "buyers," who set up shop under a legitimate name.[24] The Western Express defendants allegedly exchanged Eastern European currency for prepaid cards for which Western Express functioned as both the load location[25] and the distributor.[26] The defendants also communicated with the criminal participants utilizing carding websites devoted to trafficking in stolen credit card information and personal identifying information.[27] When the authorities searched the residences of the owners, they found over $100,000 on prepaid cards loaded in denominations of under $1,000 each to divert suspicion.[28]

SVCs also have been involved in cases involving criminal prosecutions. In 2007, Horacio Munar, an Argentinean citizen, was convicted of fraud and money laundering for a scheme involving stolen checks.[29] The checks were cashed in the United States, the proceeds were then transferred to SVCs, and the funds were later withdrawn at ATMs in Argentina and Uruguay.[30] In 2008, Sallie Wamsley-Saxon, her husband, and several others were indicted in Charlotte, North Carolina, for running a prostitution service.[31] Court documents allege that Mrs. Wamsley-Saxon used SVCs issued by Green Dot Corp. to transfer funds and to pay for the prostitutes' hotel expenses.[32] In October 2008, Behcet Alkis, a U.S. resident of Turkish descent, was convicted of money laundering and fraud in a

20. *Id.*
21. *Id.*
22. Claburn, *supra* note 18.
23. News Release, New York County District Attorney's Office, Manhattan District Attorney Robert M. Morgenthau Announced Today the Indictment, Arrest and Extradition of Viatcheslav Vasilyev and Vladimir Kramarenko for Global Trafficking in Stolen Credit Card Account Numbers, Cybercrime, and Identity Theft (Aug. 31, 2009) [hereinafter Western Express Indictments], *available at* http://manhattanda.org/whatsnew/press/2009-08-31.shtml.
24. Claburn, *supra* note 18.
25. Sienkewicz, *supra* note 16.
26. *Id.*
27. Western Express Indictments, *supra* note 23.
28. Sienkiewicz, *supra* note 16.
29. News Release, U.S. Dep't of Justice, Nov. 26, 2007, *available at* http://www.justice.gov/usao/ohn/news 2005-2009/26November2007.html.
30. *Id.*
31. Nathan Vardi, *Cash Is King*, FORBES, Apr. 7, 2008, at 36.
32. *Id.*

scam that he and his wife conducted over the course of over five years.[33] Mr. Alkis and his wife, through identity theft and Social Security fraud, obtained multiple false identities that they used to open credit card accounts and P.O. Box accounts. They would use the credit cards, develop payment histories until the account limits were raised, then max the cards buying SVCs, ultimately abandoning the accounts to charge-offs.[34] The Alkises bought SVCs from their own mall kiosk as well as from other merchant retailers.[35] Mr. Alkis was prosecuted for fraud and money laundering and ultimately received forty months in prison and was ordered to pay $802,713 in restitution.[36] His wife was sentenced to five years of probation and ordered to pay back $230,120 to the credit card companies involved.[37] Finally, David Murcia Guzman, a Colombian businessman operating a holding company known as DMG Group, which permitted customers to buy prepaid cards that they were able to then use to buy retail items, was shut down.[38] The business model permitted existing customers to "sign up" new customers to the prepaid card service, which enabled the existing customers to earn points that were loaded onto the cards and redeemable as cash.[39] Although authorities suspected that DMG Group was involved in more nefarious activity—namely laundering profits from drug trafficking—they were unable to generate sufficient proof upon which to build an indictment.[40] What was alleged, however, was that DMG was able to funnel narcotics proceeds through the catalog business by "using the Colombian Black Market Peso Exchange . . . to launder illicitly-obtained dollars in the United States, in exchange for pesos taken in for legitimate purchases [namely purchases made by customers of DMG in its catalog] in Colombia."[41] DMG operated for five years before being shut down in January 2009 for operating a Ponzi scheme.[42]

The operations of Western Express were, at least at first glance, far more complex than the others. The "Western Express Cybercrime Group"—as it is titled in the indictment—had a structure that consisted of four levels of anonymous transactions: "vendors," "buyers," "money movers," and "cybercrime services

33. Byran Denson, *Lloyd Center Kiosk Operator Sentenced for Financial Fraud*, OREGONLIVE.COM (Oct. 2, 2008), http://www.oregonlive.com/news/index.ssf/2008/10/lloyd_center_kiosk_operator_se.html.

34. *Id.* A charge-off is an account that was not paid to the extent that the creditor has internally listed it as a loss for tax purposes. It does not mean that the creditor will no longer attempt to collect the amount that is owed. *See* BLACK'S LAW DICTIONARY (9th ed. 2009).

35. Denson, *supra* note 33.

36. *Id.*

37. *See id*.

38. Press Release, U.S. District Attorney Southern District of New York, Oct. 23, 2009, *available at* http://www.justice.gov/usao/nys/pressreleases/October09/cedielrozoluisfernandoarrivalpr.pdf.

39. *Id.*

40. *See id*. at 2–3.

41. *Id*. at 2.

42. *See id*.

providers."[43] The vendors sold misappropriated personal identifying information and credit card numbers to buyers.[44] The buyers used the Internet to purchase that information for purposes ranging from re-shipping scams, larceny, and identity theft, to the more mundane phishing and spamming.[45] Cybercrime services providers then aided the potential buyers with their purchase of "stolen credit card numbers and other personally identifying information through various computer services that they provided to the vendors and the buyers."[46] Finally, the money movers—Western Express is allegedly in this category—provided financial services and conducted transactions for other "participants in the criminal enterprise" by laundering funds through prepaid cards, digital currency, such as WebMoney and E-Gold, and wire transfers.[47] The scheme was so complex and involved so many layers of anonymity that, while the indictment itself was a product of the Manhattan District Attorney's Office and the Secret Service, the actual legwork—which took upwards of two years—was conducted by agents of the New Jersey Electronic Crimes Task Force; agents of the U.S. Drug Enforcement Administration's (DEA) New York Field Division; DEA agents from around the world; the Department of Justice's Office of International Affairs; and the Ministries of Justice, Prosecutors Offices, and law enforcement agencies of Greece, the Ukraine, and the Czech Republic.[48] By contrast, the Arbuckle indictment, which took less than a year and involved investigations by only two agencies, the DEA and the U.S. Attorney General's office, was made much more transparent by two major factors: 1) Mr. Arbuckle never bothered to register Moola Zoola as a money-transmitting business (MSB) and was therefore unlicensed in all states in which he did business; and 2) Moola Zoola transferred and transmitted funds that were derived from an immediately traceable criminal offense (the PayPal scam).[49] Overall, the scams have ranged from the mundane (Moola Zoola) to the overly complex (GMG Group). But one thing remains: the availability of prepaid systems with few guidelines, and even less enforcement, makes them an attractive alternative for money launderers—one that regulatory regimes in both the United States and the European Union have failed to adequately address.

II. THE U.S. REGULATORY REGIME

In general, there are four major systems for SVC purchases: closed, semi-closed, semi-open, and open.[50] Closed system gift cards are the basic, branded,

43. *See* Western Express Indictments, *supra* note 23.
44. *Id.*
45. *Id.*
46. *Id.*
47. *Id.*; Sienkiewicz, *supra* note 16.
48. Western Express Indictments, *supra* note 23.
49. Ellis, *supra* note 11; Sienkiewicz, *supra* note 16, at 17.
50. Furletti, *supra* note 4, at 2.

retailer-issued gift cards, and they are issued and redeemable only directly from a retailer; for example, a Starbucks gift card.[51] These cards are generally sold in pre-set dollar amounts and in many cases, though this is changing, are not reloadable.[52] Semi-closed system cards are those that are issued by third parties; e.g., banks and payment processing companies.[53] They are generally embossed with the logo of a branded card network, such as Visa or American Express, and can generally be issued and used within a specified group of multiple merchants and run in the same way as a major credit card.[54] Semi-open cards, on the other hand, while very similar by virtue of how they are issued and redeemed, are generally accepted wherever major credit cards are accepted.[55] Finally, open system gift cards are essentially the same as semi-open cards with the added functionality of allowing the cardholder to use the card at an ATM and withdraw cash that has been deposited onto the card.[56]

The United States has focused much of its SVC legislation in the area of consumer protection.[57] In 2005, however, the government released an official report documenting its concern regarding the money laundering threat that prepaid SVCs posed, titled *The Money Laundering Threat Assessment* (MLTA).[58] The study presented evidence of significant weakness in the U.S. regulatory scheme that would permit money launderers to exploit the U.S. financial system. One of the highlighted areas was prepaid SVCs.[59] In most cases, due to the virtually anonymous nature of the transactions, it becomes difficult if not impossible to trace money transfers made through SVCs,[60] and the report details shortcomings that are specific to SVCs, including the cross-border features that allow users to use cards issued inside of the United States on foreign soil and vice versa.[61]

The market of "unbanked" consumers, the payment processing firms would argue, is rife with those who would prefer anonymity in their transactions. The fact that the manufacturer and servicer of the card generally has absolutely no contact with the end user—most of these cards are sold and resold like any other commodity—means that it would become cost inefficient for the servicing firms to enact what is tantamount to a "know your consumer" policy at this stage in the game.[62] Many firms oppose regulation that would force sellers of reloadable

51. *Id*. at 2–3.
52. *Id*. at 2.
53. *Id*. at 4.
54. *Id*.
55. Furletti, *supra* note 4, at 6–7.
56. *Id.* at 8.
57. *See, e.g.*, 12 C.F.R. § 563.27 (2007); Section 5 of the Federal Trade Commission Act (codified and amended at 15 U.S.C.A. § 45 (West 1997 & Supp. 2007)).
58. Sienkewicz, *supra* note 16.
59. *Id.*
60. *Id*.
61. *Id.*
62. *See* U.S. DEP'T OF TREASURY, U.S. MONEY LAUNDERING THREAT ASSESSMENT 2005 at 7–23 (2005) [hereinafter U.S. MONEY LAUNDERING THREAT ASSESSMENT],

cards—or at least cards that can be loaded with over a certain dollar limit—to identify and document the buyer.[63]

A. Evolution of SVCs in the United States

The first SVCs were primarily used by metropolitan transportation systems and colleges during the 1970s; prepaid phone cards followed in the early 1980s; and in the 1990s, traditional merchant gift cards evolved and the National Banking Act (NBA) authorized banks to engage third-party companies to market and sell prepaid SVCs.[64] Closed-loop cards, developed by merchants to increase customer loyalty, were the first major type of prepaid "gift cards," followed by open loop cards, which were initially used primarily by the government to replace paper-based food assistance.[65]

Efforts to regulate SVCs were initially moderate, and for many years there was a complete absence of regulation that was specifically applicable to prepaid cards as opposed to banking, credit cards, and general financial regulation.[66] The initial focus of most, if not all, SVC legislation was consumer protection oriented.[67] Since 2002, there have been major developments in laws regulating gift cards, though most state laws target issuers' terms, such as expiration dates, dormancy and service fees, disclosures and reporting requirements, while federal law tends to focus on increasing the security of the

available at http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf.

63. *Id.*

64. Kathleen L. DiSanto, *Down the Rabbit Hole: An Adventure in the Wonderland of Stored-Value Card Regulation*, 12 J. CONSUMER & COM. L. 22, 23 (2008); Blum, *supra* note 4, § 2. In 1996, the Office of the Comptroller of the Currency (OCC) issued several opinions in which it held that nationally chartered banks may issue stored value products. *See, e.g.*, OCC Interpretive Letter No. 731 (July 1, 1996), *available at* http://www.occ.gov/static/interpretations-and-precedents/july/int731.pdf.

65. DiSanto, *supra* note 64, at 23. Government-managed programs have used SVCs to transmit child support payments, unemployment insurance, and worker's compensation. 12 C.F.R. §§ 205.1-22 (2007). Federal Emergency Management Agency (FEMA) also distributed SVCs to Hurricane Katrina Victims. Press Release, U.S. Dep't of Treasury, U.S. Treasury Urges Waiver of ATM Surcharges for Katrina Evacuees (Sept. 9, 2005), http://www.treasury.gov/press-center/press-releases/Pages/js2707.aspx.

66. Christopher Woods, *Update on Prepaid Card Laws and Regulations*, 61 CONSUMER FIN. L.Q. REP. 815, 815–16 (Winter 2007).

67. DiSanto, *supra* note 64, at 23.

cards.[68] Because banking is primarily in the federal sphere, federal law on the subject has preempted many state laws regulating SVCs.[69]

Although the money laundering threat associated with prepaid SVCs has been acknowledged, it has yet to be categorically addressed. With the inception of the Patriot Act of 2001, Congress attempted a massive overhaul of the regulatory structure of U.S. financial institutions, especially cross-border transactions.[70] Title III of the USA Patriot Act is the International Money Laundering Abatement and Financial Anti-Terrorism Act; its purposes include preventing, detecting, and prosecuting international money laundering and the financing of terrorism; providing a clear national mandate for subjecting those foreign jurisdictions and financial institutions that pose particular, identifiable opportunities for criminal abuse to special scrutiny; and ensuring that all appropriate elements of the financial services industry are subject to appropriate requirements of reporting potential money laundering transactions to the proper authorities.[71]

In 2005, when the U.S. Department of the Treasury initially issued the MLTA, the major source of cross-border financial fraud in the United States, and the number one addressed threat in the last few years, was wire transfer fraud through companies such as Western Union and other money transmitting businesses.[72] The Money Laundering Control Act of 1986, updated in 1991, cracked down on banks and financial institutions by increasing reporting requirements, especially for funds being transmitted out of the country or in bonds, sending many money laundering outfits scurrying to less traceable wire transfers.[73] With the update in the regulations for the money transmitting businesses that occurred post-September 11, 2001, and with the anonymity, availability, and widespread acceptance of open system gift cards, many of these same operations are moving toward prepaid SVCs as an even more anonymous form of money laundering.[74]

The United States has three major regulatory schemes under which abuse of prepaid SVCs may be regulated and prosecuted. The Bank Secrecy Act (BSA) and the Patriot Act are most used, however. The National Banking Act, 18 U.S.C. § 1960, which is commonly used to regulate money laundering through wire

68. *See, e.g.*, H.B. 2591, 24th Leg., 2008 Sess. (Haw. 2008); A. 11034, 2008 Leg., 231st Sess. (N.Y. 2008); H.B. 3897, 105th Gen. Assemb., 2d Sess. (Tenn. 2008); 25 U.S.C. § 6809; 12 C.F.R. § 205.2(b); *see generally* Blum, *supra* note 4.

69. *See generally* SPGGC, LLC v. Blumenthal, 505 F.3d 183 (2d Cir. 2007) (holding that Connecticut's expiration date ban was preempted by the National Banking Act (NBA), but upholding its ban on inactivity fees); Goldman v. Simon Prop. Grp., Inc., 31 A.D.3d 382 (N.Y. App. Div. 2006).

70. *See* Patriot Act, *supra* note 10, §§ 301–377 (2001).

71. *Id.*

72. *See* U.S. DEP'T OF JUSTICE, NAT'L DRUG INTELLIGENCE CTR., NATIONAL DRUG THREAT ASSESSMENT 2007 at 24 (2006), *available at* http://www.usdoj.gov/ndic/pubs21/21137/; U.S. MONEY LAUNDERING THREAT ASSESSMENT, *supra* note 62.

73. *See, e.g.*, H.R. Rep. No. 102-28, pt. 1, at 38 (1991) (explaining that money launderers had begun to avoid banks and to use money transmission services).

74. Sienkiewicz, *supra* note 16.

transfers, is also a useful tool for creating civil liability for retailers, processors, or banks. Section 1960, which was enacted in 1992 and provided more extensive oversight of NBFIs than the meager protections afforded consumers through the BSA, was strengthened with the implementation of the Patriot Act's expansive banking regulations.[75]

1. The Bank Secrecy Act (BSA)

The Bank Secrecy Act's primary enforcement mechanism, the Currency and Foreign Transactions Reporting Act,[76] requires that reports and records of cash, negotiable instruments, and foreign currency transactions must be reported 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."[77] Even prior to 1992, the BSA authorized the Secretary of the Treasury to issue regulations requiring, inter alia, non-bank financial institutions such as money transmitters and currency exchangers to keep certain records and file reports,[78] but it was not clear—until the Patriot Act's amendments to the BSA—that it provided any affirmative duty for banks and their licensee third party prepaid card issuers to record and report information regarding transactions occurring through prepaid and independent non-bank money transmission networks.[79] The U.S. Department of the Treasury's Financial Crimes enforcement Network (FinCEN) has specified what types of businesses qualify as "money transmitters" or "money service businesses" and requires that each business falling into the specified categories register with FinCEN and comply with BSA regulations. Issuers of prepaid SVCs are currently covered under the BSA's reporting requirements.[80] BSA also requires financial institutions to keep records

75. *See* Courtney J. Linn, *One-Hour Laundering: Prosecuting Unlicensed Money Transmitting Businesses Under 18 U.S.C. § 1960*, 8 U.C. DAVIS BUS. L.J. 138 (2007).

76. 12 U.S.C. §§ 1829b, 1951–59; 31 U.S.C. §§ 5311–22.

77. 12 U.S.C. § 1829b.

78. FinCEN: Proposed Amendment to the Bank Secrecy Act Regulations—Requirement of Brokers or Dealers in Securities to Report Suspicious Transactions, 66 Fed. Reg. 250 (Dec. 31, 2001) (to be codified at 31 C.F.R. pt. 103), *available at* http://www.fincen.gov/statutes_regs/frn/pdf/brokerdealersar.pdf (proposing rules that were ultimately adopted in the sweeping overhaul of the Banking Secrecy Act).

79. The financial services industry, law enforcement, and regulators interchangeably refer to non-bank money-transmitters as money remitters, wire remitters, and wire transmitters. Money remitters such as Western Union and MoneyGram constitute one of five categories of what regulators mean when they use the collective term "money transmitting business." The other four subcategories of "money service businesses" (MSBs) are: 1) currency dealers or exchangers; 2) check cashers; 3) issuers of traveler's checks, money orders, or SVCs; and 4) sellers or redeemers of traveler's checks, money orders, or SVCs. 31 C.F.R. §§ 103.11(uu), (vv) (2010).

80. *Id.*

of currency transactions over indicated dollar amounts, to report currency transactions of more than $10,000 into or out of a financial institution, and to disclose certain accounts that U.S. citizens and residents hold at foreign financial institutions.[81] Suspicious Activity Reports (SARs) are a tool employed by financial institutions and law enforcement authorities to improve the odds of detecting illicit layering transactions.[82] The BSA requires that banks file SARs when they are a party to a transaction of $5,000 or more, "and the bank knows, suspects, or has reason to suspect that the transaction involves funds derived from illegal activities" or "the transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage."[83] Records of SARs must be maintained on file for inspection by the Treasury Department and IRS.

The BSA imposes civil and criminal penalties on money-service businesses covered by its regulations or individuals who fail to file a report of a deposit, money transfer, or wire over $10,000.[84] The penalties, however, are discretionary, and there are few proactive investigations into reports that are actually filed, except where MSBs fail to catch or file reports on transactions—called structured transactions—that have been broken up by a single depositor or transmitter into two or more transactions that exceed the $10,000 threshold.[85] Because the BSA is structured to flag and catch only transactions or groups of transactions totaling $10,000, thousands of transactions that implicate activity from money laundering to terror financing will be missed. Therefore, although the BSA is very useful in discouraging more "innocuous" transactions such as funds transfers to tax shelters, criminal activity is unlikely to be deterred, especially where the financial threshold that triggers the reporting requirement is so high.[86] In 2001, the BSA's provisions were amended to require all financial institutions that were covered by the BSA to establish in-house anti-money laundering (AML) programs.[87] Each institution was required to develop, implement, and maintain an "effective AML program."[88] The BSA's primary purpose appears to be to provide a disincentive to MSBs to encourage or facilitate money laundering by shifting the

81. *Id.*

82. *See* Geoffrey M. Connor, *Banking Aspects of the USA PATRIOT Act*, N.J. L.J., Dec. 3, 2001, at 49.

83. Peter Carbonara, *Dirty Money: Terrorism Has Shed New Light on Global Money Laundering: Here's How It Works, Why It Exists and Why the Proposed Government Crackdown Could Change the Way We All Do Business*, MONEY, Jan. 1, 2002, at 90.

84. *See* 31 U.S.C.A. § 5313.

85. *See* 31 C.F.R. § 103.23(a) (2008) (requiring report of funds sent to or from the United States); 31 C.F.R. § 103.11(b) (defining "at one time" to include transactions made in conjunction with others and, if for purposes of evading reporting requirements, on more than one day); *see also* U.S. DEP'T OF JUSTICE, MONEY LAUNDERING: FEDERAL PROSECUTION MANUAL 18 (1993) [hereinafter FEDERAL PROSECUTION MANUAL] (outlining elements of criminal offense); *id.* at 32–34 (discussing "at one time" provision).

86. *See* Patriot Act, *supra* note 10.

87. Sienkiewicz, *supra* note 16, at 17.

88. *Id.*

enforcement to the least cost avoider, the banks. It is not clear that this policy has been successful, and even the Money Laundering Act of 2001, passed in conjunction with the Patriot Act, gives only ambiguous guidance in its language geared toward mandatory enactments of "know-your-customer" policies in all banking and financial institutions.[89]

Because the regulatory language of the BSA requires only that banks regulate programs that they directly oversee, in many instances they are able to outsource the regulatory and compliance aspects of most SVC activity conducted by the bank.[90] Additionally, the fact that over 70% of open system SVC programs are run through the top 5% of national banks ensures that these banks outsource most of the direct oversight, setup, and maintenance through licensed NBFIs. These NBFIs, while subject to some substantive regulation, tend to be smaller, with lower capital bases, and thus have less ability to be held liable through fines and restitution for breach.[91] Finally, the banks contractually disclaim liability, and thus, although they are the ultimate servicers for the SVCs and, in many cases, credit cards, they cannot be held liable for the action or non-action of the servicers.[92] Given the vague oversight and the lack of enforcement language, it seems likely that this regulation is not really regulation at all, and will allow banks to do what they have been doing—minimize personal loss.

2. The Patriot Act

Title III of the Patriot Act presented a dramatic overhaul of the regulatory structure of the U.S. financial system. The legislation, which was intended to be broad and virtually all-inclusive, was structured primarily to address the issue of money laundering—suddenly understood to be the financial backbone of terrorist activity—but it also affects both credit cards and SVCs, if only tangentially.[93] Although Title III was written as broadly as possible, to be applicable to the businesses participating in most forms of MSBs, it does not expressly mention SVCs, and FinCEN has acknowledged that they were not contemplated at the time the Act was crafted because they were so new and there was little information

89. Henry Christensen III & M. Catherine Pieroni, *Anti-Money Laundering Legislation and Its Impact on Gatekeepers*, 342 P.L.I. 33, 34 (2007).

90. *See* Geoffrey M. Connor, *New Anti-Money Laundering Programs Raise Scrutiny Across the Board*, N.J.L.J., July 22, 2002, at 47; Maureen A. Young, *New Developments and Compliance Issues in a Security Conscious World; Financial Privacy-Advanced Issues; Recent Developments in FCRA/FACT and BSA/AML Compliance*, *in* SEVENTH ANNUAL INSTITUTE ON PRIVACY LAW: EVOLVING LAWS AND PRACTICES IN A SECURITY-DRIVEN WORLD 347, 391 (2006); Kevin J. Funnel, *Holding a Bank's Service Providers Accountable*, 1, http://www.banklawyersblog.com/Holding_Technology_Service_Providers_Accountable_Final.pdf (last visited Dec. 31, 2011).

91. *See* Sewell Chan, *Consumer Groups Urge Regulation of Nonbank Financial Institutions*, N.Y. TIMES, Mar. 5, 2010, at B3.

92. *Id.*

93. Connor, *supra* note 90.

available as to what, if any, risks they could pose for money laundering.[94] Title III is divided into three parts, the first of which speaks primarily to strengthening banking rules against money laundering, especially on the international stage.[95] Title III, thus, attempts to address problems that arise with matters such as correspondent banking, where banks must deal with foreign firms in jurisdictions where they have no physical presence.[96] This subsection also provides the Treasury Department with a number of new discretionary powers, including the authority to designate foreign jurisdictions, foreign firms, a class of international transactions, or a type of account of particular concern in the fight against illicit finance.[97]

In the second subsection, the legislation amended the definition of money laundering to include "reverse money laundering," where proceeds of legitimate activities are used for unlawful purposes.[98] This part of the legislation also amended the definition of "financial institution," stretching it above and beyond banking to include brokers-dealers and investment firms.[99] It also presents a number of measures to improve firms' due diligence and reporting, including the forced implementation of a "know-your-customer" rule and the necessity for financial institutions to establish an anti-money laundering program.[100] Finally, it requires the licensing of informal monetary organizations, such as "hawalas,"[101] doing business in the United States or with its citizens and institutions as well as increasing civil and criminal penalties for noncompliance.[102]

The second subsection of Title III equally addresses the issue of communication between the Treasury Department, law enforcement agencies, and financial-services sector institutions.[103] Private firms have been provided with the right and obligation to share with each other potentially interesting and relevant

94. *See* Julia S. Cheney & Sherrie L.W. Rhine, *Prepaid Cards: An Important Innovation in Financial Services*, 52 CONSUMER INT. ANN. 370 (2006), *available at* http://www.phil.frb.org:80/payment-cards-center/publications/discussion-papers/2006/D2006JulyPrepaidCardsACCIcover.pdf The BSA expressly applies to banks (provisions (A) and (B) in the BSA definition of financial institution) and credit card companies (provision (L)), and could reasonably apply to nonbank card marketing companies through provision (Y), or perhaps (K) or (Z). *Id.*; 31 U.S.C. § 5312.

95. *See* Patriot Act, *supra* note 10, Title III.

96. 31 U.S.C.A. § 5314 (West 2010).

97. *Id.*

98. *See* Patriot Act, *supra* note 10, §§ 352, 355.

99. *Id.*

100. *Id.*

101. "Hawalas" are informal financial transfer systems based on a network of money brokers, primarily located in the Middle East. This money transfer system has been cited as a major source of financing for terrorism. *See* Rachana Pathak, *The Obstacles to Regulating the Hawala: A Cultural Norm or a Terrorist Hotbed?*, 27 FORDHAM INT'L L.J. 2007, 2009–10, 2026–27 (2004).

102. *Id.*

103. *Id.*

information pertaining to money laundering cases.[104] Additionally, SARs sent to FinCEN are now to be available to intelligence agencies.[105]

The massive changes to U.S. financial regulation contained in Title III were primarily aimed at banking institutions. Even though the Patriot Act in its updates to the BSA and the Currency and Foreign Transactions Reporting Act extended the definitions of MSBs to include many previously uncovered NBFIs, much of the regulatory burden and enforcement action has been focused on banking institutions and money transmitters.[106] For banks and like institutions, covered transactions have become more transparent due to the requirement that each bank must create a specific Customer Identification Program (CIP).[107] The CIP must collect, at minimum, the customer's name, date of birth, and some identification number, but unfortunately the regulation still applies only to banks, savings institutions, credit unions, and similar banking organizations.[108] For NBFIs, most of the reporting requirements mandate reporting of only transactions over a certain dollar amount, generally $1,000, and most prepaid products are designed to fall well below the threshold. They, therefore, are not qualified as an MSB and are not regulated by the BSA's record-keeping requirements or FinCEN's registration requirement.[109]

Title III, much like the BSA, was never enacted to regulate electronic transactions occurring through NBFIs.[110] This has left a huge hole in regulation and enforcement of transactions occurring through NBFIs, such as small money-transmitting businesses, and issuers and redeemers of open system SVCs.[111]

3. 18 U.S.C. § 1960

Enacted in 1992 as part of the Annunzio-Wylie Money Laundering Act, §1960 was the primary tool by which the scope of federal money laundering legislation was extended to encompass NBFIs.[112] Section 1960 originally was enacted to supplement state and federal regulation of money transmitting businesses, many of which were operating without state licensure and were passing through significant amounts of unaccounted for and illegally laundered monies.[113] The Patriot Act amended § 1960 to add the stipulation that an MSB can violate § 1960(b)(1) by 1) operating an MSB that affects interstate or foreign

104. *Id.*
105. *Id.*
106. *See generally* 31 C.F.R. §§ 103.121(b)(2)(i)(1–4), 103.122–23 (2006).
107. *Id.*
108. *Id.*
109. Woods, *supra* note 4, at 217.
110. *See* U.S. MONEY LAUNDERING THREAT ASSESSMENT, *supra* note 62.
111. *Id.*
112. Courtney J. Linn, *One-House Money Laundering, Prosecuting Unlicensed Money Transmitting Businesses Under 18 U.S.C. § 1960*, 8 U.C. DAVIS BUS. L.J. 138 (2007).
113. *Id.*

commerce in any manner or degree and "otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense . . ."; or 2) operating an MSB that affects interstate or foreign commerce in any manner or degree and "otherwise involves the transportation or transmission of funds that "are intended to be used . . . to promote or support unlawful activity."[114]

This changed the existing regulatory framework in several ways. First, by making it a crime to transport the proceeds of a crime from one place to another inside the boundaries of the country, which was previously not criminally actionable, § 1960(b)(1) allows for the prosecution of transportation crimes in the cases of MSBs that "knowingly" handle criminal proceeds or money intended to fund criminal activities.[115] Second, outside of laws regulating international money laundering, most money laundering statutes do not reach "reverse money laundering" transactions (transactions that are intended to conceal the future use of money to finance crime, regardless of whether the funds themselves are proceeds of a crime).[116] Third, each of the money laundering statutes contains a requirement that a defendant must have done more than merely conduct a financial transaction using funds that he knows are the proceeds of a crime. Section 1956 requires that the defendant act with the intent to 1) conceal or disguise the crime proceeds or 2) to promote the carrying on of a specified unlawful activity.[117] And, finally, whereas under general money laundering statutes, the government must prove that the funds involved in the offense derive from a "specified unlawful activity" as defined in a list of inclusive activities, § 1960 requires that the funds derive from any "unlawful activity," not "specified unlawful activity."[118]

The 2001 amendments to § 1960 make it the most potent piece of anti-money laundering legislation because it dilutes the intent requirement for violations. Instead of the government having to prove that the prosecuted entity had knowledge that there was a licensing requirement of which they were in violation, the government must prove only that the MSB was operating without registering or receiving licensure from either the state or federal government.[119] Also, the 2006 amendments made § 1960 violations, including money laundering, a predicate crime under 18 U.S.C. § 1961(1) (RICO).[120] A predicate crime is any act or series of acts upon which a racketeering prosecution may be based, and

---

114. 18. U.S.C. §1960(b)(1) (West 2006).

115. *Id.*

116. *See* Stefan D. Cassella, *Bulk Cash Smuggling and the Globalization of Crime: Overcoming Constitutional Challenges to Forfeiture under 31 U.S.C. § 5332*, 22 BERKELEY J. INT'L L. 98, 99 (2004) (discussing reverse money laundering).

117. 18 U.S.C. § 1956.

118. 18 U.S.C. § 1960(b)(1)(C).

119. *See* Patriot Act.

120. *See* 18 U.S.C. § 1956(c)(7)(A) (2006) (defining term "specified unlawful activity" to include "[a]ny act or activity constituting an offense listed in section 1961(1) of this title except an act which is indictable under subchapter II of chapter 53 of title 31 [the BSA]").

RICO (the Racketeer Influenced and Corrupt Organizations Act), was enacted to combat organized crime by providing for stiffer penalties for acts performed as part of an ongoing criminal enterprise.[121] The effect here is that while a violation of § 1960 is not per se a BSA crime, a violation of the registration prong is analogous to other BSA violations and could be prosecuted under the BSA.[122]

All three regulatory schemes work interchangeably to affect prosecutions for money laundering, but none of them has been updated to include any type of reporting requirements that are separate and distinct for "online transactions," such as loading and redemption of SVCs. Regulations affecting banks have been more thorough and far-reaching than attempts to regulate NBFIs, which have, for the most part, remained under the radar, with the exception of the licensing and registration requirements for money transmission businesses.[123] In 2001, it was unclear whether SVCs would pose a threat at all, and very little if any thought was given to potential regulatory regimes. It is now clear, however, that there is massive work to be done, and the joint regulation that was passed to implement the reporting requirements that are currently applicable to federal banks should be amended to include open and semi-open system gift cards to close yet another avenue for potential money launderers.

B. Overview of U.S. Prepaid Card Programs

There are several levels of interaction in the operation and management of any prepaid card program: issuers, program managers, processors, banks, payment networks, and distributors.[124] Issuers are generally only banks, and some of the primary issuers of prepaid cards include Bank of America, PNC, JPMorgan Chase, and Citibank.[125] Program managers own the SVC program, and generally establish relationships with banks, payment networks, and distributors.[126] Additionally, they tend to design, market, and service the individual cards, as well as keep account records of card loads and reloads.[127] Processors verify that funds are available for individual transactions and transfer the funds into established pooled accounts.[128] Distributors sell the cards directly to the consumer and/or

121. *See* 18 U.S.C. § 1960.

122. *Id.*

123. Linn, *supra* note 112.

124. U.S. DEP'T OF JUSTICE, NAT'L DRUG INTELLIGENCE CTR., 2006-R0803-001, ASSESSMENT: PREPAID STORED VALUE CARDS 2 (Oct. 31, 2006). [hereinafter NDIC ASSESSMENT].

125. Chris Brown et al., presentation materials, Identifying and Mitigating the Money-Laundering Risks of Emerging Technologies: Prepaid, E-Card, and M-Payments, for the Money Transmitters Regulators Association Annual Conference (Sept. 4, 2009), *available at* http://www.mtraweb.org/amc/archives/presentations/2009/Minimizing-Money-Laundering-Risks-Emerging-Technologies.pdf.

126. *Id.*

127. Sienkiewicz, *supra* note 16, at 14.

128. NDIC ASSESSMENT, *supra* note 124.

provide for re-loadability through a kiosk, face-to-face location, web address, or voice center.[129] Banks maintain pooled accounts, settle payments, and issue branded SVCs, though banks also may function as program managers and/or distributors.[130] What differentiates SVC programs from credit and debit card programs is that third parties, such as program managers and distributors (including money services businesses), run them instead of one entity—usually a bank—that handles each level of the card's functionality.[131] A program manager is a third-party firm that sells the card directly to the consumer or provides the location or other channels (e.g., Internet, voice centers) through which the card can be reloaded. While these third-party firms may play a critical role in the business model for network-branded prepaid cards, their participation also may pose risks to the card-issuing banks. The program managers and distributors tend to perform the functions of processing and distributing the individual cards.[132] As such, they are regulated more strictly; most are required to register with FinCEN as MSBs and are required, under FinCEN, to have compliant customer due diligence policies. Unlike traditional credit cards or money lending, program managers and distributors generally do not have any front-end interaction with the customer. No funds are stored, and no credit-reporting is undertaken. Further, because there is no liability or chance of default, as these are prepaid services, program managers have little or no incentive to monitor the transactions. According to the Network Branded Prepaid Card Association, there are around fifty federal laws or regulations that apply to network branded prepaid cards.[133] The next section will discuss the industry responses to the money laundering prosecutions that were noted in Section I.

1. Industry Response

In most examples of prosecution related to SVC cards, third-party distributors or program managers are involved, and there is a bank card issuer who is held liable for the actions of the third party.[134] Although branding networks, Visa and MasterCard, have issued internal anti-money laundering guidelines for prepaid cards, they do not actively police the programs to ensure compliance.[135] Additionally, because banks are generally the issuers and bear the ultimate risks for "rogue players" in their distributor or program manager sphere, banks and financial institutions have become increasingly more astute when it comes to

129. Sienkiewicz, *supra* note 16, at 14.

130. *See id.*

131. *Id.*

132. NETWORK BRANDED PREPAID CARD ASS'N, MAJOR MISCONCEPTIONS ABOUT NETWORK BRANDED PREPAID CARDS AND MONEY LAUNDERING RISKS 2 (Sept. 6, 2007) [hereinafter NBPCA REPORT].

133. *Id.*

134. Sienkiewicz, *supra* note 16, at 14.

135. NDIC ASSESSMENT, *supra* note 124, at 5.

implementing compliance measures for monitoring these entities.[136] And, again—because governmental entities have increasingly allowed banks latitude in how the regulations are enforced—the Office of Thrift Supervision's "supervisory expectations for [banks'] gift card programs" contains fairly little concrete guidance outside a requirement that banks conduct "appropriate due diligence."[137] That being said, however, GCs at most large issuing banks have recommended a slate of AML procedures aimed to protect the bank's interests by imposing registration and reporting requirements for program managers and distributors for which the bank provides issuing and settlement services.[138] Because of a concerted effort by U.S. regulatory agencies to force banks and other issuing financial institutions to take responsibility for regulating gift card program managers and distributors, banks increasingly attempt to contract themselves out of liability for financial liability for fraud or other intentional crimes conducted by program managers and distributors of its prepaid products through indemnification.[139] Banks, however, can enforce indemnification provisions only where they themselves are compliant with AML/BSA guidelines for monitoring activity on their own platforms.[140] An industry of "compliance professionals" has been formed to address banks' unease over the amount of risk that they bear where fraud or other financial crimes occur.[141] Compliance professionals help banks keep abreast of changes and modifications of regulatory policy and what procedures must be implemented to keep the financial institution compliant.[142] Overall, however, because the guidelines provided by the AML and BSA are so ambiguous, it becomes increasingly difficult for banks to know and understand

136. *See id.*; *see generally* PIERRE-LAURENT CHATAIN ET AL., PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING: A PRACTICAL GUIDE FOR BANK SUPERVISORS (2009).

137. Memorandum, Office of Thrift Supervision, Gift Card Programs, *available at* http://files.ots.treas.gov/480932.pdf (last visited Dec. 31, 2011).

138. *See* Christensen & Pieroni, *supra* note 89, at 38.

139. *See, e.g.*, Merchant Gift Card Program Set Up Form, www.accept-credit-cards.com/pdfs/valuetec_setup.pdf (last visited Feb. 28, 2011) ("Indemnification. VCS and Merchant agree that they shall each indemnify and hold harmless the other party and its officers, directors and shareholders, from any and all loss, cost, expense, claim, damage and liability (including attorney's fees and court costs) paid or incurred by any one or more of them, to the extent it arises from, is caused by, or is attributable to (i) the failure by such party or its representatives to abide by the provisions of this Agreement; (ii) the violation by such party or its representatives, of any applicable laws, regulation or court order relating to this Agreement; or (iii) gross negligence, willful misconduct or any act or omission by such party or its representatives.").

140. *See* FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, BANK SECRECY ACT/ANTI-MONEY LAUNDERING (2000).

141. Sienkiewicz, *supra* note 16, at 3; Press Release, Promontory Financial Group, Anti-Money-Laundering Expert Promontory Compliance Solutions Spotlights Risk Management Strategies at Premier Conference (May 19, 2009), *available at* http://www.reuters.com/article/pressRelease/idUS187604+19-May-2009+BW20090519.

142. Sienkiewicz, supra note 16, at 3.

what their responsibilities are for regulating their MSBs.[143]

These ambiguities caused many banks to simply close MSB accounts and refuse to service them.[144] The industry response was to lobby Congress, leading to the introduction of the Money Services Business Act of 2008, which eliminates the monitoring requirements associated with accounts held by MSBs and allows MSBs to "self-certify."[145] This Act is currently being revived for consideration; it passed the House on June 23, 2008, but has yet (as of December 2011) to get out of Committee, and the Senate has never voted on the bill.[146] Congresswoman Carolyn Maloney, a Representative of the State of New York and the Chair of the Financial Institutions and Consumer Credit Subcommittee of the House Financial Services Committee, was a sponsor of the bill and has been a vocal proponent of the bill's passage.[147] Additionally, the bill was backed by Rep. Barney Frank (D-Mass.), Chairman of the full Committee, Rep. Spencer Bachus (R-Ala.), Ranking Minority Member of the full Committee, and Rep. Judy Biggert (R-Ill.), Ranking Minority Member of the Subcommittee.[148]

C. Current U.S. Regulatory Regime

There is no guarantee that the 2008 MSB will pass. Furthermore, it is doubtful that it is still necessary because most banks and financial institutions have instituted the minimal compliance and due diligence requirements necessary to effectively thwart attempts to hold them personally liable for fraud conducted on or by their MSBs.[149]

The Credit Card Accountability Responsibility and Disclosure Act (CARD Act) was signed by President Obama on May 22, 2009. Section 503 of the Act requires FinCEN, in consultation with the Department of Homeland Security, to issue final rules on the sale, issuance, redemption, or international

143. *See Regulatory Efficiency and Effectiveness*, FINANCIAL CRIMES ENFORCEMENT NETWORK, U.S. DEP'T OF THE TREASURY, http://www.fincen.gov/statutes_regs/bsa/bsa_effectiveness.html (last visited Dec. 31, 2011) [hereinafter FINCEN].

144. *See id.*

145. Press Release, Office of Rep. Carolyn Maloney, Reps. Maloney, Bachus Introduce the "Money Service Business Act" (June 17, 2009), *available* at http://maloney.house.gov/index.php?option=content&task=view&id=1870&Itemid=61.

146. Money Service Business Act of 2008, H.R. 4049, 110th Cong. (1st Sess. 2007), *available at* http://financialservices.house.gov/markup110/h.r._4049.pdf.

147. Press Release, MSB Coalition, House Financial Services Committee Moves Bill to Address National Problem of Termination of MSB Bank Accounts (June 24, 2008), *available at* http://www.fisca.org/Content/NavigationMenu/NewsViews/PressReleases/2008PressReleases/Releasemark-upofbankdiscontinuancebill62408FINAL.pdf.

148. *See* H.R. 4049.

149. FINCEN, *supra* note 143. Additionally, some compliance management firms have developed software to allow banks to monitor card usage to detect fraud and/or suspicious activities in "real time." Sienkiewicz, *supra* note 16, at 19.

transport of SVCs.[150] The final rules were issued in February 2010.[151] The current state of the regulatory regime for SVCs is muddled, but in 2009, FinCEN began the process of updating its rules for MSBs to provide clarification.[152] The proposal, according to an ABA source, is designed to:

> [U]pdate existing rules to help clarify which entities are covered by the definition of a money service business (MSB), more clearly delineate the scope of businesses covered, ensure certain foreign-based MSBs with a presence in the United States are subject to BSA rules and requirements, incorporate past guidance on MSBs into the text of the regulations, and reflect developments in technology, business operations and new products and services . . . In addition, the proposal would combine the elements that apply to stored value into one category . . . .[153]

Currently, banks have considerable leeway in regulating SVCs and prepaid products, which operate as an issuer or settlement clearinghouse. Moreover, in many cases, they are not comfortable exercising their power due to the ambiguities in the existing regulatory language.[154]

The U.S. system likely progressed so quickly and became so prominent due to the overall effects of deregulation in the financial marketplace. State reluctance to enact restrictive legislation, coupled with the tendency of federal courts to strike down state law as preempted by the NBA,[155] which was so vague as to gift cards that it constituted no regulation at all and created a thriving financial sector in pre-paid products. The states, however, have stepped up their regulation—with little interference from federal courts—in the wake of the financial crisis.[156]

---

150. The Credit Card Accountability Responsibility and Disclosure Act of 2009, Pub. L. No. 111-24, 123 Stat. 1734 (codified as amended in scattered sections of 15 U.S.C.).

151. *Id.*

152. *See generally* Letter from Robert G. Rowe, III, Vice-President/Senior Counsel, Center for Regulatory Compliance, to FinCEN (Sept. 9, 2009), *available at* http://www.aba.com/NR/rdonlyres/DC65CE12-B1C7-11D4-AB4A-00508B95258D/62383/MSBLetter090909.pdf.

153. *Id.* at 1.

154. *Id.* at 11–13.

155. *See, e.g.*, *SPGGC*, 505 F.3d. at 191–92 (finding that a seller of prepaid gift cards issued by a national bank that was a member of the VISA payment network sufficiently alleged that the state gift card law might be preempted by the NBA in certain circumstances); Amer. Bankers Assoc. v. Lockyer, 239 F. Supp. 2d 1000, 1022 (E.D. Cal. 2002) (finding that a state statute requiring credit card issuers to provide "minimum payment" warnings and disclosures in their monthly billing statements significantly interfered with the national banks' powers under the NBA and was thus preempted).

156. *See, e.g.*, Mwatembe v. TD Bank, N.A., 669 F. Supp. 2d 545, 554–55 (E.D. Pa. 2009) (Pennsylvania law governing marketing of gift cards and their disclosure

III. THE EUROPEAN REGULATORY REGIME

In Europe, by contrast, banks have generally been cautious about offering SVCs, mainly due to the failure of prior stored-value concepts (such as Mondex).[157] Banks also have concerns about their ability to charge consumers for prepaid cards, but non-banks have been fairly successful in marketing prepaid products to large retailers as an alternative to gift vouchers. The European Union provides a compelling contrast to the U.S. system because the European Union has pursued a different regulatory course, and demand for SVCs has remained quite low.[158] The European Union has directed its member countries to regulate electronic money according to its E-Money Directive. The European Commission estimated that the total amount of electronic money circulating in Europe increased from 675 million Euro in 2005 to 1,053 million Euro in 2007.[159] Many European countries now think that the Directive, which appears to have stifled the growth of SVCs in the European market, may have been too restrictive.[160]

There are a variety of factors that have contributed to the slow growth of the alternate payment sector in the European Union, including: payment culture, financial institutions, markedly different business strategies adopted by firms seeking to promote SVCs to European Union companies, and cultural indifference. The primary difference, however, seems to be the E-Money Directive, which was implemented to promote the growth of electronic money, but presents an unnecessarily complex and convoluted set of regulatory requirements for banks and financial institutions, and prevents NBFIs from participating in the market at all.[161] Additionally, the rigid capital requirements gave most financial institutions

---

requirements did not conflict with the NBA or OCC regulations authorizing national banks to issue gift cards, or significantly interfere with the national banks' gift card business, and thus was not preempted by federal law; state law did not impose duplicative or overlapping requirements on federal banks, and there were no federal regulations controlling the marketing of gift cards or directing what disclosures national banks had to provide in connection with cards.).

157. *See* Russell Brown, *Anderson: The Unmaking of Mondex*, COMPUTERWORLD NEWS WIRE (May 12, 1997), *available at* http://www.efc.ca/pages/media/nz-computerworld.12may97b.html.

158. *MasterCard Launches Guide*, *supra* note 6; *Evaluation of the E-Money Directive, Final Report* 2000/46/EC, at 22 (Feb. 17, 2006), *available at* http://ec.europa.eu/internal_market/bank/docs/e-money/evaluation_en.pdf.

159. Anita Ramasastry, *Nonbank Issuers of Electronic Money: Prudential Regulation in Comparative Perspective*, *in* CURRENT DEVELOPMENTS IN MONETARY AND FINANCIAL LAW 663, 668–69 (International Monetary Fund ed., 4th ed. 2005).

160. Impact Assessment Accompanying the Draft Proposal for a Directive of the European Parliament and of the Council Amending Directive 2000/46/EC on the Taking Up, Pursuit of and Prudential Supervision of the Business of Electronic Money Institutions: Summary of the Impact Assessment, EUR. PARL. DOC. (COM 627) 2–4 (2008), http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2008/sec_2008_2573_en.pdf.

161. *See The Electronic Money Directive: Recapitulation and Outlook* (Ass'n of E-Money Institutions in the Netherlands, Working Paper, 2003), *available at*

pause.[162] The recent calls for a regulatory overhaul strongly suggest that the European Union is currently over-regulating SVCs, is aware of it, and is attempting to correct the issue.[163]

A. History of Stored-Value Cards in the European Union

The market first produced stored value and prepaid products in the early 1990s, which provoked immediate responses from European central banks and ministries to begin regulating.[164] Before proposing or enacting any legislation, the European Monetary Institute chartered a report that determined that multipurpose SVCs—which at the time included only closed and semi-closed system cards—were "institutions which receive deposits," and, as such, it urged, only "credit institutions" should be permitted to issue electronic money.[165] The Institute was primarily concerned with private issuers "over issuing" electronic money and subsequently facing liquidity risks similar to those experienced by traditional credit institutions because the business of SVCs was, in its eyes, equivalent to deposit-taking.[166] The Institute reasoned that prepayments made to issuers were usually taken and invested, and an unsound investment policy could jeopardize the consumer's prepaid funds.[167] Lastly, the report urged, if SVCs and e-money become valid substitutes for cash transactions, the failure of any issuer could affect the stability of payment markets.[168] Most E.U. countries heeded the Institute's warnings and instituted regulatory policies that tended to limit the ability to issue any electronic money to credit and banking institutions and required issuers to maintain deposit insurance.[169] Following the pushback from financial institutions and the subsequent slow in SVC proliferation in Europe, [170] the European Commission proposed a directive that reflected the Commission's desire to provide a legal framework that would encourage innovation while providing the

---

http://74.125.155.132/search?q=cache:MWAeoDXcDA8J:www.simonl.org/docs/pp221103.doc+The+European+electronic+money+institution+and+gift+cards&cd=8&hl=en&ct=clnk&gl=us.

162. *Id.*

163. *See id.*

164. *Evaluation of the E-Money Directive*, *supra* note 158, at 18.

165. EUROPEAN CENTRAL BANK, REPORT ON ELECTRONIC MONEY 13–20 (Aug. 1998), *available at* http://www.ecb.int/pub/pdf/other/emoneyen.pdf.

166. *Id.* at 13–15.

167. *Id.* at 15.

168. *Id.* at 21–23.

169. *Id.*

170. "The Ministry of Economic Affairs did not subscribe to this point of view and formulated a minority position in the end report of the joint regulatory working group. Their position was that in order for innovation and competition to thrive, non-banks should also be allowed to issue electronic money products." *Electronic Money Directive*, *supra* note 161, at 3 n.2.

requisite safeguards for depositors.[171] In the United Kingdom, the regulation did not allow a similar interpretation of the law, because of the different local definitions of banking and credit institutions. The U.K.-based e-money company, Mondex, produced a legal opinion that clearly outlined that it could not be viewed as a credit institution under the U.K. bank regulation. "Therefore, by the looks of it, the United Kingdom was to become the country from where any e-money company would want to start doing business."[172] The ECB, on the other hand, concluded that the only feasible way to regulate SVCs and electronic money would be to implement the Institute's original suggestion of limiting issuance to credit institutions.[173]

The European Union has had significant success tracking and monitoring SVC transactions due to more stringent limitations on the types and kinds of institutions that can be set up to operate as money transmitting businesses.[174] The E-Money Directive reflects both the positions of the European Commission and the ECB in its guidelines.[175] It also creates an entirely new form of institution, the Electronic Money Institution (ELMI), which can also issue electronic money.[176] The requirements of ELMIs include: 1) that investments be no less than the institution's outstanding financial liabilities to its SVC depositors; 2) that redeemability be "at par value"; 3) activities restricted to those related to outstanding electronic money; and 4) a capital base of at least one million Euros.[177]

---

171. *Evaluation of the E-Money Directive*, *supra* note 158, at 19.

172. *Electronic Money Directive*, *supra* note 161, at 3.

173. *See* EUROPEAN CENTRAL BANK, *supra* note 165, at 13–20.

174. *See* FINANCIAL ACTION TASK FORCE [FATF], MONEY LAUNDERING & TERRORIST FINANCING VULNERABILITIES OF COMMERCIAL WEBSITES AND INTERNET PAYMENT SYSTEMS 26 (2008), *available at* http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf. Because the emergence of e-money occurred largely before the solidification of the European Union, regulation has varied widely among member states, though most adopted a much more proactive stance to regulation of e-money transactions. *See* Council Directive 2000/46, art. 9, 2000 O.J. (L 275), 39–43, *available at* http://ec.europa.eu/internal_market/bank/docs/e-money/evaluation_en.pdf; Directive 2009/110, of the European Parliament and of the Council of 16 September 2009 on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions Amending Directives 2005/60/EC and 2006/48/EC and Repealing Directive 2000/46/EC, 2009, O.J. (L 267) art. 18, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF.

175. *Evaluation of the E-Money Directive*, *supra* note 158, at 20. The Directive also reflects the European Commission's desire to create "a level playing field between electronic money institutions and other credit institutions issuing electronic money" by balancing the "less cumbersome features of the prudential supervisory regime applying to electronic money institutions" with "provisions that are more stringent than those applying to credit institutions, notably as regards restrictions on the business activities which electronic money institutions may carry on." Council Directive 2000/46, rec. 1, ¶ 11, 2000 O.J. (L 275).

176. Council Directive 2000/46, art. 1, 2000 O.J. (L 275), *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:275:0039:0043:EN:pdf.

177. *Id.* arts. 3–7.

The major difference between these regulations and those that were proposed by SVC issuers and watch groups is the issue germane to the regulations: ELMIs must still be certified and regulated in a manner vastly similar to "credit institutions."[178] Credit institutions in the European Union are equivalent to U.S. banks; they are licensed and regulated by the government, and they have minimum capital requirements, capital ratios, and "fit and proper" requirements.[179]

The E.U. SVC system is markedly similar to the U.S. system in that the E.U. system still has multiple tiers of involvement, with banks as required issuers, processors, and program managers.[180] The overall effect of the requirement that SVCs be distributed and maintained by credit institutions has been to drastically limit the proliferation of SVCs in the European market by restricting the proliferation of semi-open and closed card systems of the type that pioneered the gift card market in the United States.[181] Overall, however, in most of the E.U. countries, there is no recognizable difference between ELMIs and credit institutions, although there are some minor differences in the "sound and prudent" operation requirements for ELMIs.[182]

Most E.U. states differentiate little or not at all between ELMIs and credit institutions. But, in at least two countries, ELMIs are required to submit monthly reports.[183] On the other hand, the United Kingdom has recently implemented a secondary regulatory system to account for the risk differentials between credit institutions and ELMIs, which may produce a marked increase in the development of the market in the U.K.[184]

The effects of the core requirements for ELMIs that have been instituted on SVC providers have varied by state. The overall changes affected capital requirements, limitations of investments, redeemability, and restrictions on activities.[185] The expanded capital requirements may further contract the ELMI market, but there are different principles regulating the amount and types of investments that can be made with deposits.[186] Perhaps the largest barrier to the proliferation of ELMIs in many E.U. member states has been the effect of the conflicting waiver requirements for certain small e-money schemes, such as closed system non-reloadable gift cards, as implemented within the member states.[187] Finally, the last source of regulatory tension for implementation and establishment

178. *Id.* art. 1(4).

179. *Opinion of the European Central Bank on the Taking Up, Pursuit, and Prudential Supervision of the Business of Electronic Money Institutions*, 2009 O.J. (C 30) 2–4, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:030:0001:0009:EN:PDF.

180. *See* Part II.B. *supra* for a discussion of the processing levels for SVCs in the United States.

181. *Id.*

182. *Evaluation of the E-Money Directive*, *supra* note 158, at 51–52.

183. *Id.* at 24.

184. *Id.* at 86.

185. *Id.* at 99.

186. *Id.*

187. *Evaluation of the E-Money Directive*, *supra* note 158, at 99.

of EMLIs has been the anti-money laundering regulations.[188]

B. Evolution of the E.U. Regulatory Regime

Currently, electronic money in the European Union is divided into two broad categories: card-based and server-based. The primary difference between these two is not always patently clear, but it allows an analysis both of the existing market and the logic and rationale underlying the E.U. regulations. In a server-based system, the customer and the merchant do not keep the e-money in devices held in their possession. The e-money is stored in customer and merchant accounts on servers accessed via the Internet. The customer and merchant sub-systems are therefore software processes running on the central server.[189] Server-based money is complex, not fully regulated, and not currently fully reported. Regulation varies widely, and there are few clear-cut rules to define reporting. Overall, few member states report the numbers of their server-based systems, and when they do, the guidelines are often inconsistent; i.e. some countries report the total amount of e-money issued, while others report the amount of e-money outstanding, and still others report the total assets of issuers. Additionally, e-money issuers, under the ELMI and credit institution guidelines, prefer to be secretive regarding the amount of e-money that is issued, due to the stringent capital requirements.[190] Card-based money is very similar to an SVC: e-money in a pre-set value that is held by the customer on a card.[191]

Member states have struggled to implement the Directive, with several granting "grandfather" status to institutions that previously were issuing SVCs and other forms of e-money in violation of the Directive.[192] Several countries implicitly expanded the waiver requirements by raising the limits for waiver.[193] In the Netherlands, for instance, the Ministry of Finance and De Nederlandsche Bank formally stated that no change of laws was required to implement the EMI-policy stance. The issuance of pre-paid, multi-purpose, payment cards could, under the current legislation, be considered to constitute a banking activity.

At that point in time, the market also saw many new Internet-based e-money products being introduced in the course of an overall Internet-hype. The first Internet banks came into existence, and credit-card companies started working together to make safe payments over the web a reality. Meanwhile regulators were implementing the ELMI-policy stance, leading to a diverse regulatory landscape. Germany, France, and Spain implemented the ELMI-policy position through actual changes in legislation.[194] The Netherlands did not change the laws but

188. *Id.*
189. *Id.* at 75.
190. *Id.*
191. *Id.*
192. *Evaluation of the E-Money Directive*, *supra* note 158, at 75.
193. *Id.*
194. *Id.*

limited the issuance of electronic money by applying existing bank supervisory legislation. Belgium and Austria did not worry, as the issuers of electronic money were in fact all banks. The U.K. remained the country where no bank license was needed to be operational.[195]

C. Current E.U. Regulatory Regime

The European Union, while understandably hesitant to adopt the U.S. stance that problems could be dealt with as they arose, has begun a widespread deregulation of ELMI and other credit institution e-money providers. The overall goals of the regulatory shift were to: 1) create an equal playing field; 2) encourage cross border e-money transactions; 3) ensure the overall stability and soundness of issuers; and 4) increase consumer confidence in e-money products.[196]

As far as creation of an equal playing field is concerned, during the period of transition in which European currency was being converted and the ECB was attempting to regulate uniformly across member states for banking fees, terms, requirements, and "exchange fees," the issue of e-money was addressed because of the issues that the ECB encountered in standardizing the currency. Additionally, the fact that there were many existing closed and open systems that operated on the states' pre-existing currencies and that states had fundamentally different banking systems created a prioritization issue, making it unlikely that e-money issues would shore up the forefront of the debate.[197] Overall, the primary concern for equality has been the assurances that cross-border transactions are not incurring punitive fees and/or unnecessary delays in transmission. The fact that, at least prior to the Directive, many Eurozone states had laws in place to regulate e-money within their borders posed another problem. The drafting and implementation of the Directive was a feat unto itself.[198] The hope that electronic Euros, which could be spent Europe-wide, would be introduced has not been fulfilled. Cash has been faster than e-money. On the Internet, traditional means of payment such as credit cards, direct debits, or payment on delivery are dominating. Finally, in areas such as e-loyalty (cards specific to a particular brand or merchant), regulation may have been increased. This raises the question as to the current options for policy makers. A lighter regulatory approach may be advisable in view of the fact that regulation often triggers circumvention. In fact, periods of financial innovation have already been described as almost entirely triggered by moves of market players who wanted to circumvent regulation.[199] In the field of payment, at least as far as software-based solutions are concerned, a relatively easy strategy to avoid

195. *Id.*
196. *Id.*
197. *Evaluation of the E-Money Directive*, *supra* note 158, at 75.
198. *Id.*
199. *Id.*

regulation within the European Union would be to offer e-money payment services from outside the European Union.[200]

D. Anti-Money Laundering Laws

With regard to anti-money laundering laws, the approaches vary, at least in theory. The E.U. regulations specifically mandate that member states create their own enacting legislation locally, but that has not always been met with enthusiasm.[201] In the U.K., the FSA has adopted a pragmatic approach to money laundering. The FSA tries to apply the guidelines elaborated by the Joint Money Laundering Steering Group in a proportionate way to ELMIs and waived institutions.[202] In practice, the identity of the customer does not need to be verified up front (when the e-money account is opened or the card bought), but only if and when the e-money is withdrawn/redeemed or the total turnover on an account exceeds €5,000. The identity of a merchant accepting e-money must always be verified.[203] Belgium and France also have specific rules that specify the conditions under which e-money cards and accounts can be anonymous; i.e., the identity of the customer does not need to be verified. These are a maximum storage capacity of €150 (in both countries), and in France, a limit of €30 per individual transaction.[204] In Italy, the purse limit for anonymous e-money instruments was set at €500.

All other member states reported that, in principle, they apply the same anti-money laundering rules to ELMIs and waived institutions as they do to banks. These essentially amount to the requirement to ascertain the identity of customers when an e-money account is opened or an e-money card bought, and there is a need to perform checks and follow up on unusual transactions. However, to what extent these rules can be or are actually applied in practice is sometimes not clear, especially with regard to cards that are in principle anonymous. Since most member states do not have any ELMIs or waived institutions in their jurisdictions, there may not have been a need to specify rules.

The member states that do have experience with e-money issuers often acknowledge that in practice, pragmatic approaches are sometimes better suited

200. *Id.*

201. Directive 2005/60 of the European Parliament and of the Council of 26 October 2005 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing, 2005 O.J. (L 309) 22, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:EN:PDF; *see also Report from the Commission 27th Annual Report on Monitoring the Application of EU Law (2009)*, § 9.2.5.4, SEC (2010) 1143 final (Jan. 10, 2010), *available at* http://ec.europa.eu/eu_law/docs/docs_infringements/annual_report_27/sec_2010_1143_en.pdf.

202. *Evaluation of the E-Money Directive*, *supra* note 158, at 3.

203. *Id.* at 68.

204. *Id.*

than a full and immediate application of all rules. The Czech and Danish authorities reported that there was no need to identify the customers of e-money cards in their countries. In Germany, rules are negotiated with each ELMI applicant. It was also pointed out that ELMIs and waived institutions in Germany can apply for an exemption from the money laundering rules; several entities had applied, but no general exemption had been granted.[205]

Many national authorities also emphasized the importance of Directive 2005/60/EC on the prevention of the use of the financial system for money laundering and terrorist financing, which gives member states a legal basis for applying a risk-based approach to money laundering.[206] This directive allows member states the option not to apply customer due diligence in respect of products where there is clearly a reduced risk of money laundering, including e-money "where low limits are imposed on the amount issued, the amount that can be stored on an electronic device or the size of the permitted transactions." In practice, this is expected to mean that issuers will not be required to verify the identity of their customers until the total turnover on an e-money account exceeds €2,500.[207]

However, industry stakeholders find that in cases where the identity of customers does need to be verified, there are differences as to what methods of verification are acceptable to the authorities in different member states. For example, in the U.K., some forms of electronic verification are possible, but in Germany, they are not. Verification requirements in the Netherlands are said to be stricter than those in the U.K. According to the only ELMI licensed in Germany, compliance with anti-money laundering rules was the main problem area during the application process, which took fifteen months.[208] German and U.K. banks initially did not want to allow anonymous accounts, but eventually agreed to a solution similar to the general rules in France and Belgium: for anonymous accounts, the total account balance limit is €150, the limit for a single transaction is €30, and the limit for the total volume of weekly transactions is €150. This is an exemption from the normal rules, subject to review after two years.[209] Another application for an ELMI license is currently in process in Germany. The new applicant also sees money-laundering rules as one of the main problems, both in terms of the low thresholds for anonymous accounts and acceptable identity verification methods for non-anonymous customers.[210]

Some countries do not impose reserve requirements on ELMIs.[211] In most

205. *Id.* at 69.

206. *Id.*

207. *Evaluation of the E-Money Directive*, *supra* note 158, at 69.

208. *Id.*

209. *Id.*

210. *Id.*

211. *See generally Opinion of the European Central Bank on the Introduction of E-money Institutions*, CON/2004/37 (Dec. 3, 2004) (explaining a draft law amending the Act on transfers of funds, electronic means of payment, and payment systems and other laws, including the Act on Banks).

other member states, however, ELMIs are (or would be) subject to the same reserve requirements as traditional credit institutions. In some cases, national authorities with no experience with ELMIs or waived institutions were unsure which rules would be applicable.[212] For member states, the ECB's view is that it must be possible to impose reserve requirements on ELMIs and that at least all ELMIs should be treated equally.[213] Because ELMIs are generally considered a subcategory of credit institutions, they would be subject to Article 19.1 of the Statute of the ESCB, which allows the ECB to require credit institutions established in Member States to hold minimum reserves.[214] In any case, this seems to be a largely theoretical issue at present; in Germany, for example, ELMIs and waived institutions are in principle subject to the same reserve requirements as credit institutions, but in practice they are exempt due to the low volumes of business. Reserve requirements were not named as a contentious issue by any of the industry stakeholders interviewed.

Strict anti-money laundering rules are likely to have had a negative impact on the development of the market, as several industry interviewees have pointed out that restrictions on anonymous accounts are excessive. The rules that are applicable are not always clear; only two countries have explicitly specified general maximum thresholds for anonymous e-money instruments.[215] In one other, these have been negotiated during the ELMI license application process.[216] Other member states are likely to turn a "blind eye" to anonymous low-value e-money cards.[217] The most flexible approach is found in the U.K., where e-money issuers are exempted from the know-your-customer rules as long as the total turnover on an account does not exceed €5,000 or the e-money is redeemed.[218] The industry in the U.K. is satisfied with this "pragmatic" approach. Many hope that once the Third Money Laundering Directive is implemented, a similar approach will be introduced in all member states. But differences in terms of which forms of identification are considered valid for non-anonymous accounts are likely to persist. While the ECB insists that it must be possible to impose reserve requirements on ELMIs, this is not the case in a number of non-member state countries.[219] There is some degree of uncertainty among national authorities as to whether reserve requirements apply to ELMIs in some member states. However, this issue is unlikely to have had any practical impact on the development of the market, as no ELMI or waived institution in any member state

212. *Id.*

213. *Id.*

214. *Protocol (No. 4) on the Statute of the European System of Central Banks and of the European Central Bank*, art. 19.1, 2008 O.J. (C 115), *available at* http://www.ecb.int/ecb/legal/pdf/en_statute_from_c_11520080509en02010328.pdf.

215. *Evaluation of the E-Money Directive*, *supra* note 158, at 68.

216. *Id.*

217. *See generally id.* at 68–89.

218. *Id.* at 68.

219. *Id.* at 70.

has been required to hold minimum reserves.[220]

The results of the uncertainty over regulation, the strict know-your-customer requirements in place in most member states, and the reserve and transaction limitations have placed a damper on, or at least detected, money laundering in the European Union as a whole. Overall, since 1992, there have been fewer than five prosecutions for money laundering through e-money products originating in the European Union. Although this data is inconclusive, it seems clear that a know-your-customer system is the most efficient way to ensure that there are minimal reporting issues and lower governmental workloads. House Republicans rejected a measure that would have required a know-your-customer requirement for certain types of reloadable cards with transaction limits of over $5,000, which is comparable to the E.U. system.[221]

IV. MEMBER STATES V. U.S. STATES: THE DIFFERENCES BETWEEN NONSOVEREIGN AND SOVEREIGN STATE ENFORCEMENT MECHANISMS

The European Union is comprised of completely autonomous member states and, as such, enforcement of E.U. guidelines is often disparate or completely refused. In the United States, on the other hand, federal regulations are generally upheld and enforced, even at the state court level. This section provides an overview of enacting legislation and enforcement techniques on the state level and will focus on Germany and Arizona. These regions were selected for two very important reasons: both states share borders with countries with lax financial enforcement and high financial crime, and both have been controversially proactive in combating financial crime.

Germany is one of the most proactive E.U. states; it quickly implemented the E-Money Directive as well as its own changes to banking and monetary requirements. German regulations for bank and financial institutions have strict, zero-tolerance, know-your-customer requirements that extend into the prepaid and SVC sectors.[222] Additionally, although Germany has had fewer instances of criminal prosecutions and involvements in international prosecutions for money laundering through its banks, its anti-money laundering laws are some of the strictest in the European Union.[223] Because Germany is the eastern-most Western European state and borders the Czech Republic, previously a major hub of money laundering activity in Eastern Europe, it faces substantial challenges in its banking regulations.[224]

---

220. *Evaluation of the E-Money Directive*, *supra* note 158, at 70.

221. *See* S. Amend. 1066 to H.R. 627, 111th Cong. (2009).

222. *See* Katlen Blöcker, *Reporting Suspicions of Money Laundering and Whistleblowing Under German Law*, 6 J. OF MONEY LAUNDERING CONTROL 52, 53 (2002).

223. *Id.*

224. The Czech Republic has since stepped up its AML defenses, although it has been insinuated that this was merely a show to back up its application for E.U. membership.

Although Arizona has led U.S. states in proposing regulatory changes to catch money laundering, because it is merely a state, not a sovereign country like Germany, federal law would preempt most proposed regulations. Former Attorney General Terry Goddard, however, waged independent battles with major money transmission services such as Western Union to staunch the flow of money laundering activity into and out of the state and has been vocal in noting the adaptability of money launderers.[225] Though the state won a huge battle against Western Union regarding money laundering through wire transfers, Goddard immediately warned that it "[would] not end money-laundering" and expressed concern about the upswing in the use of SVCs to supplement and in many instances replace the wire transfers.[226] Additionally, because of the nature of federal preemption, this section discusses legislation proposed by Arizona state senators to bring light to the prevalence of SVC fraud within the state. Finally, this section compares the proposals and proactive regulation taken by Germany as a sovereign state, on the one hand, and Arizona, working within an existing federal framework, on the other.

A. The German Regulatory Regime

Germany, like Arizona, suffers from a regime in which currency is interchangeable, but standards are varied, de-centralized, and often unenforceable due to general guidelines that allow member states, like U.S. states, significant leeway in enforcement. Germany initially lagged behind both the U.K. and Italy in SVC proliferation, but since 2008, more consumers have expressed interest in utilizing prepaid products and several new prepaid products have been launched.[227] Germany, taking the requirements from the E.U.'s ELMI framework, adapted it to

---

But, because it was accepted for membership, it is required to comply with E.U. guidelines for AML enforcement strategies. Arguably, this has reduced the threat of money laundering coming into Germany on the eastern front. *See* Elena Horálková, *Czech Republic to Combat Money Laundering*, ČESKÝ ROZHLAS (Feb. 14, 2002); INT'L MONETARY FUND, COUNTRY REP. NO. 04/46, CZECH REPUBLIC: REPORT ON THE OBSERVANCE OF STANDARDS AND CODES – FATF RECOMMENDATIONS FOR ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (2004).

225. Sean Holstege, *Deal Targets Wire Transfers*, ARIZ. REPUBLIC, Feb. 12, 2010, at A1.

226. *Id.*

227. News Release, MasterCard Worldwide, European Customers Turn from Cash to Prepaid for Financial Control (May 9, 2008), *available at* http://www.mastercard.com/uk/personal/en/findacard/prepaidcard/forbusiness/docs/Pan-EuroASE.pdf; *see also* Press Release, First Data Commercial Services, First Data Reveals Success Factors for Prepaid Cards in Europe (Nov. 26, 2009), *available at* http://www.firstdata.com/en_au/about-first-data/media/press-releases/11_26_09; Press Release, International Voice Cash Group, Voice Cash Issues Germany's First Prepaid MasterCard Twin-Card (Oct. 28, 2009), *available at* http://www.free-press-release.com/news-voicecash-issues-germany-s-first-prepaid-mastercard-twin-card-1256741486.html).

its existing banking regulations. The primary tools that Germany uses to regulate SVCs and monitor money laundering activities are the German Criminal Code (StGB) and the Money Laundering Law (GwG).[228] The German system, similarly to most E.U. countries and the United States, puts the onus on banks to regulate the card products for which they act as a servicer, issuer, or redeemer.[229] Banks are required to establish complex internal compliance systems that require each individual bank employee to ensure that each potentially suspicious transaction is reported. The system goes as far as to hold individual employees criminally liable if a suspicious transaction passes unreported, and the bank itself can be held civilly liable for its employees' actions.[230]

1. German Regulation of SVCs

Geldkarte, Germany's electronic purse system, has over 80 million cards in circulation.[231] This system, one of the more successful European e-purse systems, is an open-system SVC that allows transactions in locations from public transportation to McDonald's.[232] What is most notable about this system is that it seamlessly melds banking and prepaid systems by allowing individuals a choice of a debit, account-connected card, and an SVC loadable with up to £ 200.[233] Additionally, Germany was the first member state to mandate that banks alone issue open system SVCs and e-money.[234] Finally, the GwG regulates SVCs (or prepaid cards, as they are called) and, in accordance with the E-Money Directive, categorizes all institutions issuing open-system SVCs as "credit institutions" with no substantive difference from the ELMI.[235]

228. Sabrina F. Preller, *Comparing AML Legislation of the U.K., Switzerland, and Germany*, 11 J. OF MONEY LAUNDERING CONTROL 234, 239–40 (2008).

229. *See* Blöcker, *supra* note 222, at 52–53.

230. *Id.* at 54; STRAFGETESZBUCH [STGB] [PENAL CODE], Nov. 13, 1998, BGBl. I. at 3,322, § 261 (Ger.).

231. *Facts and Figures*, GELDKARTE, http://www.geldkarte.de/_www/en/pub/geldkarte/press/facts_and_figures.php (last visited Dec. 31, 2011).

232. *Id.*; Felicity Ussher, *Germans Offered Smart Way to Buy Burgers*, SILICON.COM (Aug. 17, 1998), http://www.silicon.com/technology/software/1998/08/17/germans-offered-smart-way-to-buy-burgers-11003214/.

233. *Card Types*, GELDKARTE, http://www.geldkarte.de/_www/en/pub/geldkarte/geldkarte_users/card_types.php (last visited Dec. 31, 2011); *Loading and Unloading Your Geldkarte*, GELDKARTE, http://www.geldkarte.de/_www/en/pub/geldkarte/geldkarte_users/loading_and_unloading.php (last visited Dec. 31, 2011).

234. *See* Kreditwesengesetz [KWG] [Banking Act], Sept. 9, 1998, BGBL. I at 2776, *last amended* Dec. 8, 1999, BGBL. I at 2384 (Ger.)

235. *Id.* § 1, s.11.

2. German Anti-Money Laundering (AML) Laws

German AML protections are primarily grounded in the German Criminal Code, the Money Laundering Law, the Code of Criminal Procedures, the Banking Act, and other statutes.[236] The primary legislation is set out in the GwG and implements the now familiar "know-your-customer" policies pertinent to all member states.[237] Regulated entities are also required to record certain identifying information including the name, date of birth, birthplace, nationality, and address of persons conducting suspicious transactions or transactions over €15,000.[238] Additionally, they are required to keep the records on file for at least six years.[239] Finally, although German law requires that all suspicious transactions be reported and provides for criminal prosecution of individual employees as well as civil penalties—with fines up to €100,000—for responsible banking institutions, it has no specific provisions regulating the enforcement of the sanctions.[240] This may be because Germany places more value on identifying suspicious clientele than reporting.[241] Overall, Germany's regulatory regime is quite moderate, varying between possible extremes under the E-Money Directive and the U.S. regime.

B. Arizona and SVC Regulation: The Role of Preemption in State SVC Regulation

Although most laws regulating banks would be deemed preempted by federal law, because so many SVC and prepaid cards are serviced by nonbank distributors, state laws have, for the most part, been upheld.[242] In most states, however, this leeway has generally taken the form of taxes on prepaid distributors and consumer protections.[243] Correspondingly, Arizona regulates gift cards through two main sources: taxation and criminal prosecution.[244]

In March 2009, just weeks after reaching a historic settlement with Western Union, resulting in greater accountability for wire transfers, Goddard testified before the Senate Committee on the Judiciary and discussed immediately

236. Preller, *supra* note 228, at 239.

237. *Id.* at 240.

238. *Id.* at 240–41.

239. *Id.* at 240.

240. *Id.* at 241.

241. Preller speculates that this is possibly due to the difficulty of defining suspicion, although there is no standard, i.e. "reasonable suspicion." Preller, *supra* note 228, at 241.

242. *See* 10 AM. JUR. 2D *Banks and Financial Institutions* § 111 (2009); *see, e.g.*, SPGGC, *supra* note 69.

243. *See generally* ARIZ .REV. STAT. ANN. §§ 42-5061(Q), 44-7402 (West 2009); *State Gift Card Consumer Protection Laws*, CONSUMERSUNION, http://www.consumersunion.org /pub/core_financial_services/003889.html (last visited Dec. 31, 2011).

244. *See, e.g.*, State v. Fimbres, 213 P.2d 1020 (Ariz. Ct. App. 2009).

available alternatives for money launderers.[245] He noted that SVCs presented an immediate and easily available alternative to wire transfers and noted that they were "already" in use.[246] Months after, in a *Washington Post* article, Goddard bemoaned the fact that although record advances are being made in money laundering, gift cards are still being ignored.[247] According to Goddard, the best way to regulate this activity is through coordinated regulation in the United States and Mexico, granting more authority to seize criminal assets, and, most importantly, lowering the minimum threshold of reporting single transactions. It is currently $10,000.[248]

Goddard's vocal objections to the current system raise the effect of preemption on the ability of individual states to combat criminal issues of import within their own borders. The federal government's position during the Bush era was that federal preemption laws served an important national interest; the conservative think tank American Enterprise Institute admitted that preemption served to "safeguard against unwarranted state interference with the national economy" and to stop "aggressive trial lawyers and [state] attorneys general" from increasing regulation on corporations.[249] Under the Bush administration, most consumer finance legislation was preempted, but there were no corresponding increases in the budgets of the agencies that held the newfound regulatory responsibilities.[250]

President Obama, however, began rolling back several of the most controversial of these preemptions soon after taking office.[251] Because the proliferation of open-system SVCs occurred primarily in the last ten years, it remains to be seen whether they will continue to be regulated under the NBA or returned to the states under the power to regulate consumer finance, though the CARD Act seems to preclude this result. Additionally, in a seeming nod to this administration's wariness to decentralize regulation just yet, in April 2010, Arizona Senator Gabrielle Giffords introduced a congressional bill to regulate

---

245. *Law Enforcement Responses to Mexican Drug Cartels: Hearing Before the Senate Committee on the Judiciary, Subcommittee on Crime and Drugs and the Senate Caucus on International Narcotics Control*, 111th Cong. (2009) (testimony of Terry Goddard, Arizona Attorney General) [hereinafter Goddard testimony].

246. *Id.*

247. *Outspoken; A Conversation with Terry Goddard, Attorney General of Arizona*, WASH. POST, Apr. 5, 2009, at B2.

248. *Id.*

249. Nathan Newman, *Restoring State Authority: An Agenda to Restrict Preemption of State Laws*, PROGRESSIVE STATES NETWORK (Feb. 9, 2009, 1:19 PM), http://www.progressivestates.org/node/22649; *see also* Edmund Mierzwinski, *Preemption of State Consumer Laws: Federal Interference is a Market Failure*, 6 GOV'T L. & POL'Y J. 6 (2004); *OCC's Aggressive Preemption of States' Consumer Banking Protections*, CONSUMERSUNION.ORG (July 17, 1998), http://www.consumersunion.org/finance/9171rptdc798.htm.

250. Mierzwinski, *supra* note 249 at 8.

251. Phillip Rucker, *Obama Curtails Bush's Policy of 'Preemption': It Let Federal Rules Override State Law*, WASH. POST, May 22, 2009, at A3.

SVCs more stringently.[252]

However unlikely, returning the regulatory authority to the individual states would serve two important federal interests: 1) defer to the states' view of priority issues in financial regulation; and 2) decrease the regulatory (and the corresponding financial) burden on the federal government. This is arguably why the E.U. system has been so successful. The European Union provided a regulatory directive with certain minimum standards, and member states were permitted to restrict further as their needs dictated.

V. ANALYSIS: ONGOING U.S. REGULATORY CHANGES

Although critics have stated that the load limits on SVCs make the idea of using them as a mass money-laundering tool laughable, recent criminal cases concerning SVCs as well as general law enforcement concerns belie their nonchalance.[253] The biggest change in the current U.S. regulation of SVCs occurred in May 2009 with the enactment of the CARD Act. Section 503 of the Act requires the Treasury Department to "issue regulation in final form implementing the [BSA], regarding the sale, issuance, redemption, or international transport of [SVCs]."[254]

The CARD Act notes that the major change affecting SVCs is their classification as monetary instruments.[255] This requirement, which mimics the E.U.'s classification system, would place a greater requirement on banks and NBFIs to collect, report, and store information on individual SVCs storing more than $3,000.[256] This is a departure from the previous system, which did not differentiate SVCs from other monetary instruments and had a minimum reporting requirement of $10,000.[257] Consumers, however, are still only required to file a Report of International Transportation of Currency or Monetary Instrument (CMIR) when they cross an international border carrying SVCs valued at $10,000 or more.[258]

There has been congressional debate regarding whether the new classification scheme can effectively reduce money laundering through SVCs or whether it will merely lead to restrictive regulations, invasions of privacy, and bureaucratic red tape that will create headaches for banks and well-meaning

252. H.R. 5127, 111th Cong. (2010); Devlin Houser, *Cash-Card Laundering Is Bill's Focus*, ARIZ. DAILY STAR (Apr. 24, 2010, 12:00 AM), http://azstarnet.com/news/local/border/article_d6992d70-1023-5009-9399-7298cdfba7f4.html.

253. *See* discussion *supra* Part I.B.; *Gift Cards Just the Ticket for Organized Crime*, CANWEST NEWS SERVS. (Dec. 26, 2009), http://www.canada.com/topics/finance/story.html?id=877147bf-7d4a-4784-a707-73bba550b8ab&k=10939.

254. CARD Act, H.R. 627, Title V, § 503, 31 U.S.C. § 5311.

255. *Id.*

256. *Id.*

257. *Id.*

258. *Id.*

consumers.[259] On one hand, the banking industry continues to urge that imposing new regulations and reporting requirements may chill the development of the SVC market.[260] On the other hand, however, law enforcement officials urge that they have seen and seized SVCs at border crossings, and that is sufficient indication that the cards are being used for nefarious purposes and must be substantively regulated.[261] More worrisome is the fact that, even when these cards are seized, there in most cases is no way to ascertain the value of funds stored on the cards because most SVCs do not display the value on the face of the card, and the value may be learned only by contacting the bank holding the funds.[262] This creates a nearly insurmountable obstacle because of privacy laws protecting individuals' banking records.[263] Federal agents may not, in most cases, force a bank to reveal the balance of the connected account without a warrant or subpoena.[264] And, even if technological advances allow federal agents to ascertain the balance or attempt to authorize transactions to verify the card's validity, should this be permissible in the absence of a warrant or subpoena?

Some would argue that there are less "intrusive" means by which law enforcement, at least in time-sensitive situations like border-crossings, could verify the type of SVC or card that an individual is carrying and the balance.[265] But no matter how you slice it, the bottom line is that the individual citizen or person will

---

259. *Compare* U.S. DEP'T OF JUSTICE, NAT'L DRUG INTELLIGENCE CTR., PREPAID STORED VALUE CARDS: A POTENTIAL ALTERNATIVE TO TRADITIONAL MONEY LAUNDERING METHODS 7 (Oct. 31, 2006) (proposing that prepaid cards be defined as "monetary instruments" to allow law enforcement officers to seize cards under certain circumstances and so that law enforcement agents will generally know more about which cards are being carried), *with* Mark J. Furletti, *Why Prepaid Cards Should Not Be Classified as Monetary Instruments*, PAYBEFORE UPDATE, Sept. 2007, at 1, 3–5 (noting numerous legal and operational obstacles that will make enforcing implementing regulations difficult or impractical).

260. Furletti argues that new products will be slower to the market, that issuers may simply eliminate numerous programs due to the expense of regulatory oversight, and that the industry as a whole may suffer deleterious effects. Furletti, *supra* note 259, at 3–5 n.14.

261. Goddard testimony, *supra* note 245.

262. *See* Furletti, *supra* note 259, at 3–5.

263. *See, e.g.*, *Personal Banking Records Are Private, Says Supreme Court*, ACLU OF WASH. STATE (Apr. 30, 2007), http://www.aclu-wa.org/news/personal-bank-records-are-private-says-supreme-court; *see also* H.R. Rep. No. 1383, (1978), *reprinted in* 1978 U.S.C.C.A.N. 9273, 9306; United States v. Daccarett, 6 F.3d 37, 51 (2nd Cir. 1993) ("The Right to Financial Privacy Act ('RFPA') prohibits 'financial institutions' from giving the government access to 'the information contained in the financial records of any customer' absent a search warrant, subpoena, court order, formal written request, or customer authorization."); Chao v. Cmty. Trust Co., 474 F.3d 75, 83 (3rd Cir. 2007) (The RFPA was enacted by Congress "to protect the customers of financial institutions from unwarranted intrusion into their records while at the same time permitting legitimate law enforcement activity.").

264. *Id.*; *but see* Courtney J. Linn, *Regulating the Cross-Border Movement of Prepaid Cards*, 11 J. MONEY LAUNDERING CONTROL 146, 157 (2008).

265. *Id.* at 156–58.

have his or her banking privacy invaded. What Congress must decide, then, is whether this invasion is truly warranted by the nature of the potential offense.

VI. CONCLUSION

The European Union and the United States regulatory regimes differed greatly, at least in the beginning, in certain fundamental aspects. With the passage of the CARD Act, however, and the re-classification of SVCs as monetary instruments, it remains to be seen whether the regimes will more narrowly converge. The major remaining difference between the U.S. and E.U. regimes involves the scope of the legislation, the obligations of the regulated banks and financial institutions, and the repercussions for discovered violations that have resulted in money laundering prosecutions.

The European Union's SVC system grew relatively slowly, although not for lack of effort on the part of banking and financial institutions. The widespread and inconsistent regulations made it increasingly difficult to implement a cross-border system, which often made the systems worthless with the advancement of the euro. The widespread enactment of the changes to the E-Money Directive and creation of ELMIs, coupled with standardization of AML and reporting requirements, should increase the number of licensed ELMIs and facilitate the advancement of SVC use in the European market.

Overall, the European Union placed a higher onus on banks and financial institutions and, as a result has had lower instances of pattern abuse. The German system, in particular, which attaches both civil and criminal penalties for a failure to report suspicious transactions, provides a model that the United States would have done well to implement far earlier. Though, at first glance, the U.S. system appears to be a model of success, a closer look reveals that proactive regulation could have closed several loopholes that have been enforcement nightmares for law enforcement. Particularly in the border regions, such as Arizona, the accessibility, anonymity, and transportability of SVCs should have been a signal to lawmakers that immediate regulation was necessary.

However, even with the new regulations, the loopholes are not closing quickly enough. The $3,000 reporting minimum in a border state such as Arizona, where human smuggling can cost as little as $200, is unlikely to staunch the flow of illegal funds moving in and out of the country via SVCs. Because the United States is starting retroactively, it will be difficult to force regulation where there was none, but a start may be to continue the decentralization of enforcement authority. Moreover, in the absence of cogent federal regulation, permitting state governments to regulate more restrictively in areas of higher concern could staunch abuses more effectively. Reinstating state sovereignty to regulate financial activity within its borders may be the only way to ensure that the proper level of regulatory oversight for these issuing institutions is maintained. Banks and NBFIs will fight vigorously to defeat regulation that can hold them civilly liable, and criminal liability for reporting violations is relatively unheard of in the

United States. Going forward, the United States must prioritize safeguarding the interests of its citizen taxpayers, which will impose compliance and regulatory costs upon issuing institutions. Though it will directly impact the manner in which business is conducted, it is unlikely to derail the continued success of SVCs in the U.S. market.