THE STRANGE CASE OF AMENDED AMENDMENT S.A. 1107: DID CONGRESS MISS A GOLDEN OPPORTUNITY TO ADDRESS THE MONEY LAUNDERING THREAT POSED BY STORED VALUE CARDS IN THE CREDIT CARD ACT OF 2009?

Russell P. Leino*

I. INTRODUCTION

Stored value cards ("SVCs" or "prepaid cards") allow users to access prefunded value (either stored on the card itself or in a remote database)[1] through an embedded chip, a magnetic stripe, or simply an access number and password.[2] Though SVCs can be used in a variety of contexts, they can be divided into two basic types: "closed loop" and "open loop" cards.[3] Generally, closed loop cards can only be used for a single function or at a single merchant (or group of merchants).[4] Examples include subway fare cards and retail gift cards. Open loop cards, such as those branded by Visa and MasterCard, are processed through existing payment card networks and can be used to withdraw cash at any network-accessible automated teller machine ("ATM") or at any merchant that accepts credit or debit cards for point-of-sale transactions.[5]

Given this flexibility, the market for prepaid cards has expanded

* J.D. Candidate, University of Pennsylvania Law School, 2011; A.B., Harvard College, 2005.

1. *A Summary of the Roundtable Discussion on Stored-Value Cards and Other Prepaid Products*, FED. RESERVE BD., http://www.federalreserve.gov/paymentsystems/storedvalue/default.htm (last updated Jan. 12, 2005). The Federal Reserve Board distinguishes stored-value cards (where value is stored on the card itself) from prepaid cards (where value is stored in a remote database). *Id.* This distinction is not important for purposes of this Comment.

2. U.S. DEP'T OF THE TREASURY ET AL., 2007 NATIONAL MONEY LAUNDERING STRATEGY 39 (2007), *available at* http://www.treas.gov/press/releases/docs/nmls.pdf [hereinafter NAT'L MONEY LAUNDERING STRATEGY].

3. *The Many Uses of Stored-Value Cards*, AT YOUR SERVICE (Fed. Reserve Bank of Kan. City, Kan. City, Mo.) Fall 2003, at 2.

4. NAT'L MONEY LAUNDERING STRATEGY, *supra* note 2, at 39.

5. *Id.*

rapidly. The global open loop market, which was worth $12.8 billion in 2004,[6] is expected to grow to as much as $680 billion by 2015,[7] with additional billions likely to be spent in closed loop transactions. Because SVCs can be used to gain access to the mainstream payments system without a traditional checking or credit account, card companies have been particularly aggressive in marketing SVCs to immigrants, the unbanked, and those with poor credit.[8]

These same features have made SVCs attractive to money launderers and terrorist financiers. While consumer protection advocates have criticized prepaid cards as "an expensive way to spend your own money,"[9] the various fees imposed by card providers are a small price to pay for a money launderer seeking "a compact, easily transportable, and potentially anonymous way to store and access cash value."[10] Indeed, SVCs are appealing to money launderers for a host of reasons. First, just about any type of prepaid card—open or closed loop—is susceptible to some form of money laundering scheme.[11] Even prepaid phone cards can be used to facilitate money laundering.[12]

Second, because SVCs are designed to operate outside of a traditional banking relationship, money launderers can easily obtain and reload prepaid cards anonymously.[13] This is especially true due to the wide availability of SVCs on the Internet and through lightly regulated third-party vendors like convenience stores.[14]

Third, money launderers can use prepaid cards to approximate international wire transfers without the aid of a traditional bank or money transmitter.[15] While any open loop card with ATM access can be used to send remittances (by loading funds on to the card and dropping it in the mail), many cards are specially designed to facilitate remittances.[16] Some

6. U.S. DEP'T OF JUSTICE NAT'L DRUG INTELLIGENCE CTR., PREPAID STORED VALUE CARDS: A POTENTIAL ALTERNATIVE TO TRADITIONAL MONEY LAUNDERING METHODS 6 (2006), *available at* http://www.justice.gov/ndic/pubs11/20777/20777p.pdf [hereinafter NAT'L DRUG INTELLIGENCE CTR. REPORT].

7. Maria Aspen, *Can Prepaid Bridge Debit Divide for MasterCard?*, AMERICAN BANKER, May 28, 2009.

8. NAT'L MONEY LAUNDERING STRATEGY, *supra* note 2, at 39; *Stored Value Cards: An Alternative for the Unbanked?*, FED. RESERVE BANK OF N.Y. (July 2004), http://www.ny.frb.org/regional/stored_value_cards.html.

9. Press Release, Fin. Consumer Agency of Can., FCAC Launches Pre-Paid Payment Card Guide (Oct. 19, 2006), *available at* http://www.fcac-acfc.gc.ca/eng/media/news/default.asp?postingId=225.

10. NAT'L MONEY LAUNDERING STRATEGY, *supra* note 2, at 39.

11. *Id.* at 42.

12. *Id.*

13. NAT'L DRUG INTELLIGENCE CTR. REPORT, *supra* note 6, at 4.

14. NAT'L MONEY LAUNDERING STRATEGY, *supra* note 2, at 40.

15. NAT'L DRUG INTELLIGENCE CTR. REPORT, *supra* note 6, at 4.

16. *Prepaid Cards an Emerging Threat*, CORNERSTONE REPORT (U.S. Immigration &

cards are even sold in pairs so that a party can deposit cash in an ATM in one country and a second party can withdraw the funds from an ATM in a different country.[17]

Fourth, prepaid cards can serve to dramatically lower barriers to accessing the U.S. financial system.[18] For instance, certain offshore banks allow buyers to obtain and load SVCs with unlimited value anonymously, which enables buyers to use the SVCs to make cash withdrawals at domestic ATMs and thereby skirt numerous reporting requirements mandated by federal law.[19]

Finally, the existing anti-money laundering ("AML") laws and regulations in the United States are insufficient to contain this emerging threat. There are two main problems with the current AML regime as it relates to SVCs. First, prepaid cards are not considered "monetary instruments" for purposes of the Currency and Monetary Instrument Reporting ("CMIR") requirement,[20] a provision of the Bank Secrecy Act ("BSA")[21] that imposes a reporting requirement on any person transporting monetary instruments with aggregate value of over $10,000 into or out of the U.S.[22] This means that the two criminal statutes used to enforce the CMIR requirement[23] cannot be applied to unreported or smuggled SVCs, even if the aggregate value of the cards is much higher than $10,000.[24] The result is an easily exploitable loophole whereby ill-intentioned individuals can *legally* move large amounts of money into and out of the U.S. This loophole is especially consequential because prepaid cards are already inherently less conspicuous to transport or ship than bulk cash.[25]

The second major flaw in the current U.S. AML regime as it relates to SVCs is that sellers of prepaid cards, though defined as "money services businesses" ("MSBs") under the BSA, are not required to register with the Financial Crimes Enforcement Network ("FinCEN"),[26] are not required to

Customs Enforcement, D.C.), Dec. 2006, at 4, *available at* http://149.101.23.4/doclib/news/library/reports/cornerstone/cornerstone3-2.pdf.

17. NAT'L MONEY LAUNDERING STRATEGY, *supra* note 2, at 40.

18. *See id.* (describing money laundering vulnerabilities presented by prepaid cards).

19. NAT'L DRUG INTELLIGENCE CTR. REPORT, *supra* note 6, at 5.

20. 31 U.S.C. § 5316 (2006); *see* 31 U.S.C. § 5312(a)(3) (2006) (defining "monetary instruments").

21. Bank Secrecy Act of 1970, Titles I and II of Pub. L. No. 91-508, 84 Stat. 1114-1124 (1970) (codified as amended at 12 U.S.C. § 1829(b), 12 U.S.C. §§ 1951-59, & 31 U.S.C. §§ 5311-32).

22. Courtney J. Linn, *Regulating the Cross-Border Movement of Prepaid Cards*, 11 J. MONEY LAUNDERING CONTROL 146, 151 (2008).

23. *See* 31 U.S.C. § 5324(c) (2006) (criminalizing CMIR reporting violations); 31 U.S.C. § 5332 (2006) (criminalizing smuggling of monetary instruments).

24. NAT'L DRUG INTELLIGENCE CTR. REPORT, *supra* note 6, at 3.

25. *See id.* (noting that SVCs occupy less physical space than cash).

26. FinCEN is the bureau of the U.S. Department of the Treasury charged with

retain any form of customer identification or transaction records, and are not required to file Suspicious Activity Reports ("SARs").[27] In fact, the only federal reporting requirement currently applicable to SVC providers is the filing of Currency Transaction Reports ("CTRs"), which must be completed for all cash transactions over $10,000.[28] Significantly, the subset of MSBs classified as "money transmitters"—which does not include SVC providers—must comply with *all* of the above requirements.[29] This loophole effectively eliminates the "paper trail" that is so crucial for law enforcement efforts directed at combating money laundering and other financial crimes involving prepaid cards.[30]

Given the regulatory passivity to date, it has become increasingly clear that Congress will need to take direct corrective action to eliminate these loopholes. In May of 2009, Congress had the opportunity to do just that when Senator Susan Collins introduced an amendment, S.A. 1107,[31] to legislation that eventually became the Credit Card Accountability Responsibility and Disclosure Act of 2009 ("Credit CARD Act" or "Act").[32] As proposed, S.A. 1107 would have directly addressed the two problems noted above: not only would SVCs have been defined as monetary instruments, but providers of prepaid cards would have been defined as money transmitters.[33] Thus, had S.A. 1107 been enacted as proposed, transporters of prepaid cards with an aggregate value of over $10,000 would have been obligated to file CMIR reports, and SVC vendors would have been required to verify, record, and retain customer information on all transactions over $3000 and file SARs on all suspicious transactions over $2000.[34]

However, S.A. 1107 was not enacted as proposed. One day after Senator Collins proposed the amendment, Senator Richard Shelby offered a modified version of S.A. 1107 with strikingly different language.[35] Instead

administering the Bank Secrecy Act. FED. FIN. INSTS. EXAMINATION COUNCIL, BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL 4 (2006) [hereinafter FFIEC BSA/AML EXAMINATION MANUAL].

27. NAT'L DRUG INTELLIGENCE CTR. REPORT, *supra* note 6, at 4.

28. *Id.* at 3.

29. *Id.* at 4.

30. *See infra* note 75 and accompanying text (discussing the importance of a paper trail).

31. 155 CONG. REC. S5426-27 (daily ed. May 13, 2009) (statement of Sen. Collins).

32. Credit Card Accountability Responsibility and Disclosure Act of 2009, Pub. L. No. 111-24, 123 Stat. 1734 (2009).

33. *See* 155 CONG. REC. S5415 at 5426 (modifying language of the Credit CARD Act, which would have directly modified the language of the BSA).

34. *See* NAT'L DRUG INTELLIGENCE CTR. REPORT, *supra* note 6, at 4 (discussing obligations of a subset of MSBs that are presently classified as money transmitters).

35. *See* 155 CONG. REC. S5471 (daily ed. May 14, 2009) (statement of Sen. Shelby) (modifying language of original S.A. 1107).

of directly amending the United States Code to include the relevant language about prepaid cards, the new version of the amendment directed the Secretary of the Treasury to issue regulations related to SVCs within 270 days, and noted that the Secretary "may" wish to include CMIR reporting requirements as part of such regulations.[36] The Senate unanimously accepted the amended amendment, which eventually became Section 503 of the Credit CARD Act signed into law by President Obama.[37] Senator Collins issued a press release trumpeting the inclusion of the amended amendment as a victory in the fight against drug cartels.[38]

Perhaps Senator Collins is right. However, given the relatively weak language in Section 503, the amended amendment may have actually done more harm than good by forestalling meaningful action while at the same time providing political cover to opponents of reform. Although the Department of the Treasury is required to promulgate *some* kind of regulations related to SVCs,[39] it need not enact anything in particular, and thus the existing loopholes could remain open.[40] This situation is unacceptable, especially because the introduction of S.A. 1107 was not the first time Congress proposed—but failed—to address these issues.[41] Congress should cease its equivocation and confront the flaws in the current AML regime head-on by immediately amending Section 503 with the language from the original S.A. 1107.

The remainder of this Comment will discuss these issues in greater detail. Part II will examine the origins of SVCs, how they operate, and how they are used. Part III will describe the basic processes of laundering money and financing terrorism, and how SVCs may be used in those processes. Part IV will discuss the specific money laundering threat from different types of SVCs. Part V will examine the shortcomings of the current U.S. enforcement regime for AML and the prevention of terrorist financing as it relates to SVCs. Part VI will set forth the arguments others

36. *Id.*

37. Credit Card Accountability Responsibility and Disclosure Act of 2009, Pub. L. No. 111-24, 123 Stat. 1734, § 503 (2009).

38. Press Release, Senator Susan Collins, Senate Approves Collins Amendment Restricting Flow of Drug Cartel Money (May 19, 2009), *available at* 2009 WLNR 9538049; http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MinorityNews&ContentRecord (select "May" and "2009 (85)" from dropdown menus; then follow hyperlink associated with "05/19/09").

39. Interestingly, the Department of the Treasury has apparently already missed the prescribed deadline for developing these regulations: 270 days after May 22, 2009 (the date on which the Act was signed into law) was February 16, 2010.

40. *See* Credit Card Accountability Responsibility and Disclosure Act of 2009 § 503 (including no specific requirements for regulations).

41. *See, e.g.*, Violent Crime Control Act of 2007, H.R. 3156, 110th Cong. § 338 (2007) (proposing to close CMIR loophole); S. 1860, Violent Crime Control Act of 2007, 110th Cong. § 338 (2007) (proposing to close CMIR loophole).

have raised *against* closing these loopholes, including both practical and legal objections, and then analyze and answer these counterarguments. Part VII will conclude this Comment by arguing that notwithstanding the issues discussed in Part VI, the money laundering threat from SVCs must be addressed and the best place to begin is by closing the loopholes in the current AML regime via a Congressional amendment to the amended amendment.

II. THE ORIGINS, OPERATION, AND USES OF STORED VALUE CARDS

Prepaid cards are not a new phenomenon. The first SVCs were developed in the 1970s by an Italian vending machine company frustrated by thefts of metal coins from its machines,[42] and were subsequently used in transit systems and on college campuses.[43] In the 1980s, the first prepaid phone cards emerged in the United States.[44] Then, in 1994, the luxury retailer Neiman Marcus introduced the first stored value gift card, and the first bank-issued prepaid cards came into use in 1996.[45] These closed loop cards were soon followed by open loop cards, first introduced by government agencies as a replacement for paper-based food stamps[46] and long-haul trucking companies looking for a convenient payroll solution for their itinerant drivers (who often lacked personal bank accounts).[47] Network branded open loop SVCs came next, and by 2008 there were seven million Visa or MasterCard branded prepaid cards in circulation.[48] Industry experts expect the prepaid market to continue to grow rapidly, with some analysts predicting that certain prepaid products will experience more than 100% growth per year.[49]

Network branded prepaid cards function in a manner similar to traditional debit cards. First, the cardholder swipes his card through a point-of-sale or electronic data capture terminal at a retail store or ATM.[50] The terminal reads the sixteen-digit number encoded in the card's magnetic stripe, which serves to identify the card and the issuing bank.[51] The

42. John T. Albers, Note, *Stored Value Cards: Should We Know the Holder?*, 11 N.C. BANKING INST. 363, 367 (2007).

43. Kathleen L. DiSanto, *Down the Rabbit Hole: An Adventure in the Wonderland of Stored-Value Card Regulation*, 12 J. CONSUMER & COMMERCIAL L. 22, 23 (2008).

44. *Id.*

45. *Id.* at 23 n.6.

46. *Id.* at 23.

47. Albers, *supra* note 42, at 369.

48. *Id.*

49. NETWORK BRANDED PREPAID CARD ASS'N, FREQUENTLY ASKED QUESTIONS ABOUT NETWORK BRANDED PREPAID CARDS 2 (2007) (on file with author) [hereinafter NBPCA, FREQUENTLY ASKED QUESTIONS].

50. Linn, *supra* note 22, at 151.

51. *Id.*

terminal then transmits this information to the third-party processor of the beneficiary bank, which in turn queries the third-party processor of the issuing bank regarding whether the card is valid and whether the funds associated with the card are sufficient to carry out the transaction.[52] If the card is valid and there are sufficient funds, the issuing bank responds with an electronic "OK" and places a hold on the funds, which are generally held in a pooled account at the issuing bank.[53] When the transaction is later settled, the issuing bank reduces the available balance associated with the card by the purchase or withdrawal amount.[54] During this process, the only information actually transmitted to the merchant terminal is the approval or denial of the transaction.[55]

Because SVCs offer an alternative means of accessing the existing payments system infrastructure, it is not surprising that consumers, businesses, and governments have embraced these products with great enthusiasm. Consumers can use prepaid cards in place of traveler's checks and gift certificates, to send remittances to family members abroad, and as educational tools to teach teenagers how to manage money and use credit cards responsibly.[56] Those consumers who distrust or lack access to the traditional banking system or have poor credit can use prepaid cards in place of traditional credit or debit cards.[57]

Businesses have also seized on SVCs as convenient and useful tools. Instead of issuing traditional payroll checks, some businesses issue prepaid cards to employees and simply load money onto the cards when payroll comes due.[58] This type of SVC is especially useful for businesses in which employees are widely dispersed or constantly on the move, and use of SVCs for payroll purposes can result in lower payroll transaction costs for all types of employers.[59] Other businesses issue promotions and rebates to their customers in the form of SVCs, and some insurance companies provide claim payments to policyholders on prepaid cards.[60]

Government agencies also use SVCs, most frequently to issue benefit payments such as unemployment, child support, and food stamps.[61]

52. *Id.*

53. *Id.* The use of a pooled account rather than an account associated with a particular individual is the key difference between the operation of a prepaid card and a traditional debit card. *Id.* The ramifications of this distinction are discussed in greater detail in Part VI.

54. *Id.*

55. *Id.*

56. NBPCA, FREQUENTLY ASKED QUESTIONS, *supra* note 49, at 2.

57. Fed. Reserve Bank of N.Y., *supra* note 8.

58. NBPCA, FREQUENTLY ASKED QUESTIONS, *supra* note 49, at 2.

59. Albers, *supra* note 42, at 369-70.

60. NBPCA, FREQUENTLY ASKED QUESTIONS, *supra* note 49, at 2.

61. *Id.*

Prepaid cards have even been used for settlement payouts in government litigation, as with the $20 million settlement resulting from the Federal Trade Commission's 2007 lawsuit against pyramid-schemer SkyBiz.com.[62] Additional creative uses for SVCs by each of these groups will continue to emerge in the years to come.

III. THE BASIC MECHANICS OF MONEY LAUNDERING AND TERRORIST FINANCING

Money laundering can be defined as "the criminal process of processing ill-gotten gains, or 'dirty' money, through a series of transactions; in this way the funds are 'cleaned' so that they appear to be proceeds from legal activities."[63] While there are many different types of money laundering schemes,[64] such schemes generally involve three distinct steps: placement, layering, and integration.[65] SVCs have the potential to play a key role in all three stages, though they are likely to be most useful in the placement and layering stages.

Placement is the initial stage of money laundering. The goal during the placement stage is to introduce the "dirty" money into the legitimate financial system without attracting the attention of law enforcement personnel or the financial institutions where the transactions take place.[66] Because placement is the point in the money laundering process when illicit proceeds can most easily be traced to the underlying criminal activity, it is the stage in which the launderer is most vulnerable. As such, placement often involves dividing large amounts of ill-gotten money into smaller sums, using these sums to purchase monetary instruments at one financial institution, and then depositing or cashing the instruments at a different financial institution.[67] This type of activity, which is designed to circumvent the various reporting requirements at the targeted financial institutions, is commonly called "structuring" because the transaction is structured to avoid detection.[68] Because some types of SVCs can be anonymously purchased and reloaded,[69] and because they provide an easy

62. Press Release, Fed. Trade Comm'n, Stored Value MasterCards Sent Today to SkyBiz Pyramid Scheme Victims (May 21, 2007), *available at* http://www.ftc.gov/opa/2007/05/skybizredress.shtm.

63. FFIEC BSA/AML EXAMINATION MANUAL, *supra* note 26, at 7.

64. *See generally* NAT'L MONEY LAUNDERING STRATEGY, *supra* note 2, at 15-71 (discussing various money laundering threats).

65. FFIEC BSA/AML EXAMINATION MANUAL, *supra* note 26, at 7-8.

66. *Id.* at 8.

67. *Id.*

68. *See id.* at app. G (discussing structuring of money laundering).

69. NAT'L DRUG INTELLIGENCE CTR. REPORT, *supra* note 6, at 4.

initial access point to the U.S. financial system,[70] prepaid cards have obvious appeal as a placement tool for money launderers.

The second general stage in the money laundering process is layering. Launderers use layering to obscure the link between the underlying criminal activity and the money being laundered by moving the funds around the financial system, usually through a complex series of transactions.[71] These transactions serve to complicate the paper trail and cause confusion for anyone attempting to trace the true origin of the money.[72] Because of their portability, flexibility, and lack of regulation, prepaid cards are extremely useful for layering. In addition to the fact that SVCs are extremely compact and physically easy to ship and transport, many types of prepaid cards can be used to approximate international wire transfers without the aid of a traditional bank or money transmitter.[73] Furthermore, because of the relatively weak AML regulations on SVCs,[74] the paper trails generated by transactions involving prepaid cards are inherently less robust than those generated by transactions involving more traditional monetary instruments.[75] As one commentator observed, "[a]n internal U.S. Treasury report notes that the September 11 hijackers were later identified by their bank accounts, card signatures, and wire transfers. 'Had the terrorists used prepaid cards to cover their expenses, none of these financial footprints would have been available,' the report said."[76]

The final step in the money laundering process is integration. The goal of integration is to provide a plausible explanation for the source of the funds.[77] After the funds have been introduced into the financial system in the placement stage and insulated from the underlying criminal activity during the layering stage, additional transactions are completed to create the "appearance of legality."[78] Such additional transactions often involve the purchase and sale of real estate, securities, or other assets.[79] Another method of integration involves moving the money through the accounts of a legitimate, cash-intensive business. Certain money laundering schemes

70. NAT'L MONEY LAUNDERING STRATEGY, *supra* note 2, at 40.

71. FFIEC BSA/AML EXAMINATION MANUAL, *supra* note 26, at 8.

72. *Id.*

73. NAT'L DRUG INTELLIGENCE CTR. REPORT, *supra* note 6, at 4, 6-7.

74. *Id.* at 3-4.

75. *See* Chester Dawson, *Prepaid Cards: Candy for Criminals?*, BUSINESS WEEK, Dec. 12, 2005, at 42, *available at* http://www.businessweek.com/magazine/content/05_50/b3963115.htm (noting that prepaid card transactions fall outside the purview of federal statutes and consequently have not been subject to the types of institutional monitoring commonly applied to transactions involving traditional monetary instruments).

76. *Id.*

77. FFIEC BSA/AML EXAMINATION MANUAL, *supra* note 26, at 8.

78. *Id.*

79. *Id.*

have utilized the large-scale sale or exchange of closed loop gift cards or phone cards as a tool for integration.[80]

Unlike traditional money launderers, the goals of terrorist financiers are generally ideological rather than profit seeking.[81] Nevertheless, the actual processes used by terrorist financiers are quite similar to those used by traditional money launderers.[82] Instead of seeking to obscure the origins of illicit funds to protect their profits, terrorist financiers use similar methods to obscure their connections to terrorists or specific acts of terrorism. Put another way, terrorist financing uses the same *means* as traditional money laundering to accomplish essentially converse *ends*: while traditional money launders seek to conceal the source of funds *derived* from illicit activity, terrorist financiers seek to conceal the source of funds *used to finance* illicit activity.[83]

One key difference between traditional money laundering and terrorist financing is that funds involved in terrorist financing may come from legitimate sources, such as charitable donations.[84] Thus, terrorist financing sometimes operates in the exact opposite direction of traditional money laundering: instead of disguising criminal funds by financing legitimate activity, legitimate funds are disguised and used to finance criminal activity. Regardless of the origin of the funds and the timing of the underlying criminal act in the process, the characteristics that make SVCs useful for traditional money launderers also make SVCs useful for terrorist financiers: portability, flexibility, and anonymity. As such, the remainder of this Comment will generally not differentiate between money laundering and terrorist financing.

IV. THE SPECIFIC MONEY LAUNDERING THREAT FROM VARIOUS TYPES OF SVCS

According to the U.S. government, virtually all types of prepaid cards pose some kind of money laundering risk.[85] The most obvious money laundering risks come from general-use open loop cards and specially designed remittance cards.[86] These types of SVCs are not only compact and easily transportable, but they also serve as a potentially anonymous

80. NAT'L MONEY LAUNDERING STRATEGY, *supra* note 2, at 40.

81. FFIEC BSA/AML EXAMINATION MANUAL, *supra* note 26, at 8.

82. *Id.*

83. *See Id.* at 9 (describing methods common to both traditional money laundering and terrorist financing).

84. *Id.* at 8.

85. *See* NAT'L MONEY LAUNDERING STRATEGY, *supra* note 2, at 42 (outlining potential threats from different types of SVCs). The single exception is "function-specific cards" (e.g., transit system cards), which pose no apparent potential threats. *Id.*

86. *Id.*

way to circumvent barriers to the U.S. payment system and access ill-gotten cash at ATMs all over the world.[87] Because of their tremendous flexibility, general-use and remittance SVCs can be utilized in all three stages of money laundering, as well as in terrorist financing schemes.

SVCs designed to facilitate payroll transactions, while extremely useful for legitimate businesses, also pose a significant money laundering and terrorist financing risk,[88] particularly in the layering and integration phases of the money laundering process. Specifically, money launderers can use payroll cards issued by fraudulent businesses to obscure the origin of ill-gotten funds or to fund terrorist operations from diverted legitimate funds.[89] Given how easy it is to purchase an "off the shelf company,"[90] the fraudulent use of payroll cards is clearly a legitimate concern.

Multi-merchant gift cards also pose a money laundering risk.[91] These cards, which may be open or closed loop, can only be used for purchases of goods and services (they cannot be used to access funds through ATMs).[92] An example of a closed loop multi-merchant gift card is a gift card that can be used at any store in a particular mall.[93] Open loop multi-merchant gift cards are readily available through most major credit card companies and banks, and are generally accepted wherever the issuing company's credit and debit cards may be used.[94] Both types of multi-merchant gift cards can be easily (and often anonymously) purchased in bulk and resold,[95] thereby facilitating both the placement and layering stages of the money laundering process.

Even closed loop single-merchant gift cards and prepaid phone cards can be used in money laundering schemes.[96] These types of cards can be used in a number of different ways: as an alternative form of currency in black markets, as a cash-intensive front business,[97] or through a modified

87. *Id.* at 39.

88. *Id.* at 42.

89. *Id.*

90. *See, e.g.*, *Off the Shelf Companies / ready made companies - £54 plus VAT*, FORMATIONS DIRECT, http://www.formationsdirect.com/Offtheshelfcompanies.aspx (last updated Jan. 7, 2011) (detailing process for ordering an "off the shelf company").

91. NAT'L MONEY LAUNDERING STRATEGY, *supra* note 2, at 42.

92. *Id.*

93. *See, e.g.*, *Gift Cards*, VALLEY WEST MALL, http://www.valleywestmall.com/information/gift_cards (last visited Jan. 6, 2011) (showing an example of a closed loop multi-merchant gift card).

94. *See, e.g.*, *Debit Cards: Chase Gift Cards*, CHASE, https://www.chase.com/ccp/index.jsp?pg_name=ccpmapp/individuals/shared/page/gift_card (last visited Jan. 6, 2011) (showing an example of an open loop multi-merchant gift card).

95. NATIONAL MONEY LAUNDERING STRATEGY, *supra* note 2, at 42.

96. *Id.*

97. The sale of prepaid phone cards for use on cellular or long-distance networks is traditionally a cash-intensive business, making it an attractive integration mechanism for money launderers. *Id.* at 40.

version of the Black Market Peso Exchange, a complex system in which 1) drug suppliers sell ill-gotten dollars to currency brokers in the U.S. in exchange for Colombian pesos, 2) the currency brokers use the dollars to buy goods in the U.S., and 3) the currency brokers sell the goods in Colombia in order to generate more pesos to sell to drug suppliers in the U.S.[98] The money laundering threat associated with closed loop SVCs is well known in the law enforcement community, and FinCEN has been warning of money laundering risks associated with prepaid phone cards since at least 2001.[99] Even the popular television series *The Sopranos* featured an episode involving an illicit prepaid phone card scheme.[100]

Aware of these risks, a number of major SVC providers (including Visa and MasterCard) have attempted to establish voluntary AML programs related to SVCs, such as account limits and identity verification procedures.[101] However, even the most mainstream general-use prepaid card providers often rely on third-party marketing companies to sell their products.[102] This third-party involvement has the potential to complicate voluntary AML programs significantly, particularly with respect to identity verification.[103] Furthermore, although many mainstream SVC providers have begun to limit the amount that can be placed on any one card, a simple Internet search reveals that anonymous, no-cap prepaid cards issued by offshore financial institutions are still readily available.[104] Thus, it seems doubtful that voluntary guidelines represent a genuine solution to the money laundering threat posed by SVCs.[105]

V. THE SHORTCOMINGS OF THE CURRENT U.S. AML ENFORCEMENT REGIME AS IT RELATES TO SVCS

Combating money laundering and terrorist financing is an important

98. *Id.* at 40, 42. A detailed primer on the Black Market Peso Exchange can be found at http://www.fincen.gov/news_room/rp/advisory/pdf/advisu9.pdf.

99. *Suspicious Activity Related to Phone Card Businesses*, SAR BULL. (Fin. Crimes Enforcement Network, D.C.), June 2001, *available at* http://www.fincen.gov/news_room/rp/rulings/pdf/sarbul6-01.pdf.

100. *The Sopranos*, *Season 2-26: Funhouse–Synopsis*, HBO, http://www.hbo.com/the-sopranos#/the-sopranos/episodes/2/26-funhouse/synopsis.html (last visited Jan. 6, 2011).

101. NAT'L MONEY LAUNDERING STRATEGY, *supra* note 2, at 41.

102. Albers, *supra* note 42, at 391-92.

103. *See id.* (noting potential difficulties in verifying customer information provided by nonbank marketing companies).

104. *See, e.g.*, *Bank Account Introduction with Prepaid Debit Card*, THETABIZ OFFSHORE, https://www.offshore-services.biz/offshore-credit-card/ (last visited Jan. 6, 2011) (showing example of an anonymous no-cap prepaid card available from an offshore entity).

105. *See* NAT'L MONEY LAUNDERING STRATEGY, *supra* note 2, at 41 (noting that "[voluntary] guidance may not be consistently enforced").

priority of the U.S. government.[106] This is evidenced in part by the severity of sanctions related to money laundering: an individual convicted of money laundering can be sentenced to twenty years in prison and fined up to $500,000,[107] and any property or assets traceable to the proceeds of criminal activity may be subject to forfeiture.[108] The enforcement of these sanctions depends, however, on the ability of law enforcement officials to establish an evidentiary trail linking underlying criminal activity to particular funds. Unfortunately, the existing AML laws and regulations do not adequately address the money laundering threat posed by SVCs, and the current regime does not give law enforcement personnel the tools they need to establish the necessary paper trail when prepaid cards are involved in a money laundering scheme.

As noted in Part I, there are two major loopholes in the current AML regime as it relates to SVCs. First, prepaid cards are not considered "monetary instruments" for purposes of the CMIR statute.[109] This statute requires any person who transports monetary instruments with an aggregate value of over $10,000 into or out of the U.S. to report that they are doing so.[110] This requirement is designed, in part, to prevent bulk cash smuggling, which is a crucial aspect of the placement stage of many money laundering schemes.[111] Because large-scale international criminal enterprises such as sophisticated narcotics trafficking operations often generate massive amounts of small-denomination currency, physically moving that cash from the "scene of the crime" to a location where it is accessible to the ultimate beneficiaries of the crime (often across international borders) is a key challenge for money launderers.[112] Vehicles, couriers, and package delivery services are all commonly utilized in bulk cash smuggling operations.[113]

As with many components of the U.S. AML regime, both the underlying conduct (here the cross-border smuggling of cash) and the failure to report that conduct (here the failure to file a CMIR report) are criminalized.[114] If law enforcement personnel discover unreported monetary instruments with a total value of more than $10,000, such

106. NAT'L MONEY LAUNDERING STRATEGY, *supra* note 2, at iii.

107. 18 U.S.C. § 1956 (2006).

108. FFIEC BSA/AML EXAMINATION MANUAL, *supra* note 26, at 9.

109. NAT'L DRUG INTELLIGENCE CTR. REPORT, *supra* note 6, at 3.

110. 31 U.S.C. § 5316 (2006).

111. *See* NAT'L MONEY LAUNDERING STRATEGY, *supra* note 2, at 50-53 (discussing bulk cash smuggling).

112. *Id.*

113. *Id.*

114. *Compare* 31 U.S.C. § 5324(c) (2006) (criminalizing CMIR reporting violations), *with* 31 U.S.C. § 5332 (2006) (criminalizing smuggling of monetary instruments).

instruments can be seized immediately.[115] This provides an important incentive for legitimate transporters of bulk cash and other monetary instruments to file CMIR reports and gives law enforcement a powerful tool to interdict illicit smuggling.

Unfortunately, law enforcement personnel have no recourse when it comes to individuals transporting SVCs, even when the aggregate value of the cards far exceeds $10,000.[116] This is because the existing regulatory definition of "monetary instruments" for purposes of the CMIR statute is, at present, insufficiently broad to include prepaid cards.[117] As such, narcotics traffickers and other international criminals can *legally* move large quantities of what amounts to readily accessible cash across the U.S. border without filing CMIR reports, and law enforcement personnel lack the statutory authority to seize unreported prepaid cards.[118]

To illustrate, a commentator asks his reader to imagine a hypothetical scenario in which the reader is a passenger on an international flight departing the U.S., and the passenger in the seat next to him opens a briefcase filled with stacks of high-denomination U.S. currency.[119] Clearly, current law requires that this cash be reported, and U.S. law enforcement personnel could seize the cash if it were not reported. The commentator then asks his reader to imagine that instead of cash, the briefcase is filled with neatly bound stacks of prepaid cards, the aggregate value of which could be many times greater than the currency in the first scenario.[120] Under current law, the passenger with the briefcase full of prepaid cards would have *no* obligation to file a CMIR report. Thus, even if the case full of cards were discovered, law enforcement personnel would not have the statutory authority to seize the cards. This is even more of a problem because SVCs, by their nature, are so much more portable than hard currency, and, for obvious reasons, it is far easier to conceal a $10,000 prepaid card than it is to conceal $10,000 in cash.[121]

The second major loophole in the current U.S. AML regime as it relates to SVCs is that providers of prepaid cards do not fall within the definition of a class of MSBs called "money transmitters".[122] As such, businesses that sell SVCs have no obligation to register with FinCEN, to verify or retain any customer information, or to file SARs. Money services businesses that are presently classified as money transmitters, on the other

115. *See* 18 U.S.C. § 981(b)(2)(B) (2006) (authorizing seizure based on probable cause).

116. NAT'L DRUG INTELLIGENCE CTR. REPORT, *supra* note 6, at 3.

117. Linn, *supra* note 22, at 152.

118. NAT'L DRUG INTELLIGENCE CTR. REPORT, *supra* note 6, at 3.

119. Steve Cocheo, *Prepaid Dilemma: Industry Balances Utility of Stored-Value Cards with Risk of Abuse*, ABA BANKING J., Oct. 1, 2007, at 46.

120. *Id.*

121. NAT'L DRUG INTELLIGENCE CTR. REPORT, *supra* note 6, at 3.

122. *Id.* at 3-4.

hand, must satisfy all such requirements.[123] Sellers of SVCs must still file CTRs for cash transactions involving more than $10,000 and maintain some sort of AML program,[124] but these basic requirements are essentially toothless without regulatory oversight.

Absent such oversight, law enforcement personnel tracking money launderers are left with significant gaps in the paper trail when SVCs are involved. SARs have long been used to confirm hunches and build cases, and are increasingly being utilized to initiate investigations.[125] Furthermore, one of the reasons that SVCs are so appealing to money launderers is their potential for anonymity.[126] Without a requirement for basic due diligence by purveyors of SVCs, prepaid cards will continue to be an ideal tool for money launderers and terrorist financiers.

VI. COUNTERARGUMENTS AND RESPONSES

Because both of the crucial definitions hindering aggressive AML enforcement related to SVCs—"monetary instrument" and "money transmitter"—are contained in the language of the regulations rather than in the enabling statutes, FinCEN could have acted to close both of these loopholes long ago. So why has FinCEN failed to do so, at least so far?[127] Industry groups and commentators have raised a number of reasons for maintaining the status quo with respect to both the CMIR requirement and the definition of money transmitter. The remainder of this Comment will examine and respond to each set of objections, and then conclude by arguing that notwithstanding these counterarguments, the money laundering threat posed by SVCs must be addressed by closing these loopholes.

Critics argue that applying the CMIR requirement to SVCs is impractical for four main reasons. First, critics argue that because the CMIR is more or less a voluntary requirement, it is unrealistic to expect money launderers to declare that they are carrying SVCs valued at over

123. *Id.*

124. *Id.*

125. Elizabeth Donald & Dina M. Randazzo, *Plugging the Gaps in the U.S. Anti-Money Laundering System*, 6 U.C. DAVIS BUS. L.J. 10, 10 (2005).

126. NAT'L DRUG INTELLIGENCE CTR. REPORT, *supra* note 6, at 4.

127. FinCEN is currently exploring the possibility of including providers of SVCs in its definition of money transmitters. Amendment to the Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Money Services Businesses, 74 Fed. Reg. 22129 (proposed May 12, 2009) (to be codified at 31 C.F.R. pt. 103) [hereinafter FinCEN Proposed Rulemaking]. This proposed rule faces heavy resistance from the SVC industry. *See, e.g.*, NETWORK BRANDED PREPAID CARD ASS'N, RE: COMMENTS REGARDING STORED VALUE IN RESPONSE TO THE NOTICE OF PROPOSED RULEMAKING, RIN 1506–AA97 (2009) [hereinafter NBPCA, RESPONSE TO PROPOSED RULEMAKING] (opposing rule change).

$10,000. While true to an extent, this criticism could apply equally to any monetary instrument covered by the CMIR regime, not just SVCs. Furthermore, because the CMIR enforcement scheme criminalizes both the act and the failure to report the act,[128] including SVCs in the definition of monetary instruments covered by the CMIR would not only provide legitimate transporters of SVCs an incentive to file a report, but would also allow law enforcement personnel to seize unreported SVCs discovered in the course of the numerous searches that are regularly conducted at border crossings and in customs control areas throughout the U.S.

Second, critics argue that CMIR requirements for SVCs are impractical because even if law enforcement personnel are able to discover unreported SVCs, many prepaid cards cannot be easily differentiated from traditional debit cards (for which no report is required).[129] Indeed, most network-branded prepaid cards look virtually identical to debit cards, right down to the word "Debit" displayed on the face of the prepaid card.[130] To overcome this obstacle and prevent accidental seizures of traditional debit cards, law enforcement personnel will need some way to tell the difference between the two types of cards. This distinction is important because debit cards are generally linked to individual accounts, while prepaid cards are linked to pooled accounts. Because they are linked to individual accounts, debit cards are far less transferrable than SVCs, are subject to much greater regulation, and generally do not raise the same money laundering concerns raised by SVCs. Furthermore, the seizure of debit cards raises certain privacy issues that are not applicable to SVCs.[131]

One potential solution would be to require SVC issuers to include a label or emblem on the face of the card identifying the card as prepaid.[132] While card issuers might object that any mark intended to draw law enforcement scrutiny to SVCs may make the cards less appealing to potential customers,[133] there is no reason the identifying mark would need to be large or obvious, and this concern seems mostly theoretical.

Even if law enforcement personnel could easily differentiate between SVCs and traditional debit cards, a third practical obstacle to subjecting SVCs to the CMIR requirements is how to determine the value of a given prepaid card in order to confirm that a suspect is illegally transporting cards with an aggregate value of more than $10,000. Some have suggested establishing a special phone number for law enforcement personnel to call

128. *See supra* note 114 (criminalizing CMIR reporting violations and the smuggling of monetary instruments).

129. Linn, *supra* note 22, at 156-57.

130. *Id.* at 157.

131. These issues will be discussed in more detail *infra*.

132. Linn, *supra* note 22, at 157.

133. *Id.*

the card issuers,[134] but it would likely be more efficient for law enforcement personnel—and more cost effective for SVC providers—to equip relevant law enforcement personnel with portable card readers similar to those used by merchants at the point of sale.[135] Procuring and distributing card readers to relevant law enforcement personnel and training them on use of the readers would pose a logistical challenge for law enforcement agencies, but presumably not an insurmountable one.

The card readers could be phased in gradually, beginning with high-traffic border crossings and airports, and then eventually spreading to additional locations. Another benefit of introducing card readers is that their use might eventually obviate the need for identifying marks on SVCs: the card reader could be programmed to initially query the type of card, and then the reader would query the available balance only if the first reply signaled that the card was prepaid rather than a traditional debit card.[136]

The fourth and final practical obstacle to applying the CMIR regulations to SVCs is how to actually "seize" the funds associated with a prepaid card.[137] Simply taking physical possession of a card may not result in an effective seizure because there may be other cards that can access the same stored value.[138] In light of this, any card reader used by law enforcement personnel should also be able to initiate a debit of the attached funds, through a process similar to that used in standard merchant transactions (as described in Part II).[139] The funds could then be deposited in a special account held by the U.S. government until further proceedings were completed.[140]

Thus, the use of slightly modified existing technology could reasonably overcome the main practical objections to including SVCs in the definition of monetary instruments. However, there are also potential constitutional and privacy concerns that must be addressed. Most importantly, it must be determined whether the swiping of an SVC by a law enforcement officer to determine the card's balance constitutes a "search" under the Fourth Amendment,[141] and, if so, whether this search can be

134. *Id.* (discussing suggestion by NBPCA to utilize a 1-800 number for this purpose).

135. NAT'L DRUG INTELLIGENCE CTR. REPORT, *supra* note 6, at 8; *see also* Linn, *supra* note 22, at 157 (suggesting use of "point of sale-type device" by law enforcement personnel).

136. *See* Linn, *supra* note 22, at 157 (describing the potential process for government-generated queries of SVCs).

137. *Id.*

138. *See* NAT'L MONEY LAUNDERING STRATEGY, *supra* note 2, at 40 (noting that some providers allow multiple prepaid cards to be issued for the same account).

139. Linn, *supra* note 22, at 157.

140. *Id.*

141. U.S. CONST. amend. IV.

conducted without probable cause or reasonable suspicion.[142]

At first glance, swiping a prepaid card to determine its value seems similar to searching an electronic storage device (such as a computer's hard drive), which federal courts have generally held to be a search for purposes of the Fourth Amendment.[143] However, a strong argument can be made that swiping a prepaid card to determine its value is less like searching a computer hard drive and more "akin to a police officer initiating a check on a vehicle identification number or even a license plate," which federal courts have uniformly held does not constitute a search under the Fourth Amendment.[144]

Of course, vehicle identification numbers and license plates are, by design, in plain view.[145] Presumably, the stored value associated with a prepaid card is not. However, even assuming that swiping an SVC to determine its value is a search for purposes of the Fourth Amendment, such a search likely can nevertheless be conducted without probable cause or even reasonable suspicion. As one commentator explained, "[u]nder what is termed the 'border search' exception, routine searches of persons and the effects of entrants into the USA are not subject to any requirement of reasonable suspicion, probable cause, or warrant."[146]

This exception extends to virtually all property, including closed containers such as luggage, briefcases, wallets, purses, and the photos and papers found therein.[147] Notably, even searches of laptop computers and other electronic devices can be conducted without suspicion under the border search exception.[148] While the Supreme Court has indicated that there are some limits to the border search exception, the Court has upheld the government's right to completely disassemble and reassemble a car's fuel tank at a border crossing without suspicion.[149] Clearly, swiping a

142. *See generally* Linn, *supra* note 22, at 158-60 (discussing 4th Amendment issues related to the extension of the CMIR requirement to prepaid cards).

143. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 549 n.79 (collecting cases).

144. Linn, *supra* note 22, at 159.

145. For an object to fall within the plain view exception, the government must satisfy a three-prong test: 1) the officer must "be lawfully located in a place from which the object can be plainly seen," 2) the officer must "have a lawful right of access to the object itself," and 3) the object's "incriminating character must also be 'immediately apparent'" to the officer. Horton v. California, 496 U.S. 128, 136, 137 (1990) (internal citation omitted).

146. *Id.* at 160.

147. *See* United States v. Arnold, 533 F.3d 1003, 1007 (9th Cir. 2008) ("Courts have long held that searches of closed containers and their contents can be conducted at the border without particularized suspicion under the Fourth Amendment."); *see also* Linn, *supra* note 22, at 160 (collecting cases).

148. *See* Arnold, 533 F.3d at 1008. ("[W]e are satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border.").

149. United States v. Flores-Montano, 541 U.S. 149, 152, 155 (2004).

prepaid card to determine its value is far less intrusive than dismantling a vehicle's fuel tank, so it follows that a swipe of an SVC absent suspicion would have a strong chance of passing judicial muster under the border search exception.[150]

Another potential legal issue arising from more aggressive AML regulation of SVCs is whether swiping a prepaid card to determine its value would violate provisions of the Right to Financial Privacy Act of 1978 ("RFPA"),[151] which prohibits financial institutions from giving the government access to information in the financial records of any customer without a warrant, subpoena, court order, or customer authorization.[152] However, as one commentator has pointed out, the definition of "customer" in the RFPA is limited to a person who has "utilized . . . any service of a financial institution . . . in relation to an account maintained in the person's name."[153] Because the funds attached to SVCs are generally held in pooled rather than individual accounts, most prepaid cardholders are not "customers" for purposes of the RFPA, even though they clearly utilize the services of financial institutions.[154] As such, neither constitutional nor privacy concerns should derail a fix of the CMIR loophole as it relates to SVCs.

Turning to the issue of classifying sellers of SVCs as money transmitters, the objections are primarily practical. Most importantly, opponents of imposing FinCEN registration and other reporting requirements on SVC sellers argue that these requirements would place an undue burden on SVC vendors and would ultimately deter them from selling SVCs. This, in turn, would negatively impact unbanked customers by denying them access to the global payments system.[155] This is certainly a valid concern, particularly because many entities that currently sell prepaid cards are small, unsophisticated, and cater to markets that are underserved by more traditional financial institutions. As one commentator noted, "[u]nlike a deposit or withdrawal at a traditional bank, the cards can generally be purchased anonymously at travel offices, money-service

150. *See* Linn, *supra* note 22, at 160 (explaining that:

> A search of a prepaid card is less invasive than a fuel tank search. Not only does a fuel tank search take a significantly longer amount of time, but it involves physically probing a vehicle possessed or owned by the traveler. Swiping a prepaid card to ascertain the value of the funds associated with the card is minimally invasive, takes only a few moments, and ultimately intrudes upon information owned and possessed by a third party, not the traveler.).

151. Pub. L. No. 95-630, 92 Stat. 3641 (Nov. 10, 1978) (codified at 12 U.S.C. §§ 3401-3420, 3422 (2006)).

152. 12 U.S.C. § 3402 (2006).

153. Linn, *supra* note 22, at 161 (quoting 12 U.S.C. § 3401(a)(5) (2006)).

154. *Id.*

155. NBPCA, RESPONSE TO PROPOSED RULEMAKING, *supra* note 127.

centers or convenience stores, over the telephone or on the Internet."[156] This would "bring a whole new set of companies under the authority of financial regulators . . . the ramifications of [which] could be complex."[157]

It is worth noting in response, however, that some individual states already classify SVC vendors as money transmitters.[158] While compliance with federal regulations would likely be more burdensome than that required by existing state laws, classifying SVC purveyors in this manner is clearly not a novel concept. Furthermore, the predicted expansion of the prepaid market[159] will likely serve to mitigate the increased costs of compliance: while margins may decrease under more intensive regulation, rapid expansion of demand should more than make up for lost profits. More importantly, in light of the huge risks associated with a failure to regulate—including the possibility of a catastrophic terrorist attack akin to September 11—increased compliance costs are surely justified. At the end of the day, this burden may simply be one that "this financial community needs to bear if we're going to get a grip on money laundering."[160]

VII. CONCLUSION

The Credit CARD Act of 2009 was signed into law on May 22, 2009. As such, the Secretary of the Treasury, FinCEN, and the other financial regulators have apparently already missed their deadline to close the loopholes related to stored value cards within the 270-day timeframe set forth in the Act.[161] If the regulators fail to make the necessary changes when they issue revised regulations in the future, Congress should intervene and directly amend the language of the United States Code, as the original S.A. 1107 would have done. In order to fulfill the central purpose of the Bank Secrecy Act and "safeguard the U.S. financial system from the abuses of financial crime, including money laundering, terrorist financing, and other illicit financial transactions,"[162] Congress may have no real choice but to amend the amended amendment once again.

156. Phil Mattingly, *Card Traffic Flying Under Regulatory Radar*, CQ WEEKLY, May 25, 2008, at *2, *available at* 2008 WLNR 10362464.

157. Albers, *supra* note 42, at 393-94.

158. FinCEN Proposed Rulemaking, *supra* note 127.

159. *See supra* notes 6-7 and accompanying text (discussing expected growth of prepaid market).

160. Donald & Randazzo, *supra* note 125, at 10.

161. Two-hundred seventy days after May 22, 2009 was February 16, 2010.

162. FFIEC BSA/AML EXAMINATION MANUAL, *supra* note 26, at 7.