1998

The De Minimus Exemption of Stored Value Cards from Regulation E: An Invitation to Fraud?

Sean M. O'Connor
University of Washington School of Law

Richmond Journa l of Law &Technology

Volume V, Issue 2, Winter 1998

The *De Minimis* Exemption of Stored Value Cards From Regulation E: An Invitation to Fraud?

Sean M. O'Connor[*]

Cite As: Sean M. O'Connor, The *De Minimis* Exemption of Stored Value Cards From Regulation E: An Invitation to Fraud?, 5 RICH. J.L. & TECH. 6, (Winter, 1998) <http://www.richmond.edu/~jolt/v5i2/oconnor.html>.[**]

I. Introduction

{1} How valuable is $100? To a student? To a single unemployed parent? To a well-compensated professional? The Federal Reserve Board apparently believes that the potential loss of $100 is not a tremendous burden on anyone. In a recently proposed rule,[1] the Board exempts stored value cards[2] that contain less than $100 from the same regulations that protect consumers from most types of fraud associated with ATM, debit, and credit cards. Regulation E (Reg E) currently regulates the electronic funds transfers (EFTs) that are at the heart of ATM/debit/credit card transactions by requiring printed receipts, error resolution procedures, periodic statements, initial disclosure of terms of usage, and more.[3] Without these protections, stored value card holders will be easy targets for unscrupulous vendors who shave off an extra few pennies per transaction as well as fraudulent issuers who disburse defective cards. In short, the $100 *de minimis* exemption of stored value cards from Reg E protection is an open invitation to fraud.

{2} The Board buried this *de minimis* exemption in a detailed proposed amendment to Reg E that purports to impose modified consumer protection regulations on the rapidly expanding stored value card industry. However, the *de minimis* exemption swallows the larger rule in which it is embedded. Large financial organizations such as Visa, Citibank, and MasterCard are primarily interested in stored value cards as a means to tap into a lucrative market of low value transactions. For transactions valued at less than $20 that is estimated at $750 billion

annually in the United States alone,[4] and for transactions valued at less than $10 it is an estimated $2 trillion annually worldwide.[5] Thus, there is little desire to issue high value stored value cards that would trigger regulation anyway. In fact, industry experts already talk about "the typical $100 value limit on a stored-value card."[6] Further, the low entry costs to this enormous market, coupled with the ease of avoiding regulation afforded by the *de minimis* exemption, will attract a host of large and small investors, some of whom may capitalize on the substantial fraud potential of an unregulated and poorly understood new technology. Hints of things to come may be seen in the current proliferation and abuse of stored value cards, such as prepaid telephone calling cards.[7]

{3} While the Federal Reserve Board's stated rationale for the amendment and exemption is to balance consumer and industry interests,[8] the structure and amount of the *de minimis* exemption clearly favors card issuers.[9] Industry representatives claim that imposition of Reg E provisions, such as required transaction receipts, will make further development of the market economically unfeasible: "Premature regulation could 'impede the growth' and 'conceivably stop development' of new technologies."[10] But this is not an argument for complete exemption, rather it suggests truly modified regulations. A variation of this argument posits that legislation will "hinder competitive advantages and innovation in the industry."[11] One commentator says, "Regulations may stunt innovation because card companies would have to fit their product into a pigeon hole." [12]

{4} At the same time, the industry asserts the usual "market forces" argument that is always trotted out when consumer protecting regulations are threatened. In this case, market forces will weed out unscrupulous vendors, while word of mouth and media coverage will quickly educate consumers as to the potential dangers of these cards.[13] As Congressman Michael N. Castle argues, "[I]t would seem premature for regulations to pick winners and losers before the market is allowed to test . . . contrasting features. . . . I believe that the market will produce bargains, however Faustian, that a significant segment of consumers will choose to accept."[14] But these arguments often prove too much. Why regulate food products or drugs either, if consumers will simply boycott merchants who sell tainted products? The answer in both cases points to the level of potential harm combined with serious informational disadvantages on the part of consumers. Consumer advocates are concerned that the stored value card industry will disproportionately target and exploit lower-income groups who "do not have the resources to investigate alternatives," in the same way that many consumer loan companies and check cashing shops currently do.[15]

{5} More telling, however, is that the enabling legislation for Reg E--the Electronic Funds Transfer Act of 1978 (EFTA)[16]--is solely and expressly intended as consumer protection. The Board's balancing concern is self-imposed through its own internal Regulatory Planning and Review program.[17] Thus, the Board should instead be first and foremost concerned with protecting consumers, including those for whom $100 is a substantial amount of money. This paper proposes an alternative Reg E amendment that offers better protection for consumers while not imposing unduly harsh restrictions on a nascent, potentially useful industry. Part I describes important existing Reg E provisions in greater detail. Part II outlines the relevant aspects of stored value cards. Part III critically analyzes the *de minimis* exemption buried in the proposed Reg E amendment in light of the potential for fraud, while Part IV suggests a better compromise.

II. Regulation E

{6} Regulation E is the implementing code for the Electronic Fund Transfer Act (EFTA) of 1978.[18] EFTA was passed in response to concerns that new EFT technologies opened the door for high tech criminals ("hackers," "crackers," and "phreaks") to intercept or initiate transactions with the nightmarish possibility of wiping out someone's entire bank account with a keystroke. Thus, EFTA and Reg E provide the framework for rights, responsibilities, and liabilities of parties to EFT transactions.[19] Further, the stated primary objective of the act and regulation is to protect individual consumers who participate in EFTs.[20] Congress delegated rulewriting authority to the Board of Governors of the Federal Reserve System when it passed the Act.[21] Under the Board's current interpretation, as embodied in Reg E, EFTA covers transactions involving point-of-sale (POS) systems, automated teller machines (ATMs), direct deposits or withdrawals of funds, telephone bill-payment

plans, and transfers involving debit cards, even where not initiated through an electronic terminal.[22] However, this is not intended to be an exhaustive list.[23] The following are the important consumer protections of Reg E.

A. *Restrictions on Unsolicited Issuance of Access Cards*

{7} Unsolicited access cards may be sent, but they must be invalid, clearly marked as such, and validated only upon the consumer's oral or written request.[24] This helps prevent EFT access to individual's accounts from falling into the wrong hands, particularly where the account holder is not even aware that an access card exists.

B. *Limits on Consumer Liability for Unauthorized Transactions*

{8} Generally, consumers' liability is limited to $50 for unauthorized use of an access device as long as they notify the issuer within two days of learning of its loss or theft.[25] This provision is controversial because it can be viewed as a close policy decision regarding placing a burden on parties that have no attributable fault. By placing the burden upon the card issuer, however, Reg E gives a strong incentive for that issuer to incorporate reasonable security measures such as access codes into the system.

C. *Initial Disclosure of Terms and Conditions of EFT Service*

{9} Before the first EFT occurs, issuers must disclose the following:[26]

1. liability
2. issuer's address, telephone number, and business hours
3. types and limitations of EFTs
4. fees
5. subsequent documentation
6. stop payment procedures
7. confidentiality, and
8. error resolution procedures.

{10} In the absence of this provision, card issuers could incorporate hidden fees, liabilities, and unexpected card functions that the user would not discover until at least after the first card usage.

D. *Change in Terms Notice*

{11} In particular, changes resulting in increased consumer fees or liability, fewer available types of EFTs, or stricter limits on the frequency or dollar amount of EFTs, trigger the requirement of written notice to the consumer 21 days before the effective date.[27] Additionally, error resolution procedure notices must go out at least annually, even where no change has been made.[28] Similar to the initial disclosure requirement, this provision reduces card issuers' ability to impose hidden or surprise fees, liabilities, or functions without notice.

E. *Issuance of Terminal Receipts and Periodic Account Statements*

{12} Receipts must be made available at the time of transaction recording the amount, date, type, identification of account accessed, terminal location, and any third parties involved.[29] Periodic statements must be issued monthly where there is at least one transaction per month, quarterly if less, and contain the same information about each transaction as required for receipts.[30] Statements must also show account fees, balances, contact information for inquiries, and telephone number for preauthorized transfers.[31] This provision is the cornerstone of Reg E protection. It virtually eliminates the possibility of "black box" transactions where the user has no idea whether $10 or $100 has just been transferred.

F. *Rights Regarding Preauthorized EFTs*

{13} Preauthorized EFTs can only be established through the written request of the user; and, financial institutions must update users regarding transfer status within two business days, unless the payor has taken this responsibility.[32] Users may stop preauthorized transfers by written or oral notice at least three days before scheduled transfer; the financial institution may request that written confirmation of an oral request be submitted within fourteen days.[33] Users must receive notice of preauthorized EFTs that vary in amount, except where he or she authorizes a payment range and the variance is within that range.[34] Credit cannot be predicated on the user's acceptance of preauthorized EFT payments.[35] One can envision a variety of problematic scenarios involving preauthorized EFTs run amuck in the absence of regulation.

G. *Error Resolution Procedures*

{14} "Errors" include EFTs that are unauthorized, incorrect, omitted from periodic statements, subject to computational or bookkeeping mistakes, not reported in accordance with Reg E, or disbursed to the wrong amount.[36] Consumers have sixty days from the mailing of a periodic statement or account documentation to notify the financial institution of a possible error; the institution may require written confirmation of notice.[37] Financial institutions have ten days to investigate error allegations.[38] Then, they must report results to the consumer within three days after that.[39] And finally, the financial institution must correct the error within one business day if one has occurred where one is determined to have occurred.[40] Where the institution cannot complete its inquiry within ten days, it must provisionally credit the consumer's account, including interest where applicable, and notify the consumer of this action. The institution then has forty-five days to determine whether an error occurred, with the other deadlines remaining the same.[41] Extensions of twenty days instead of ten, and ninety instead of forty-five are permissible where the EFT was initiated out-of-state or through a POS debit transaction.[42] Where no error is determined to exist, or the error is not on the part of the financial institution, a written explanation must be issued, setting out how this was determined and what documents were used. These documents must be made available to consumer, and any debit of provisional credits must be reported to the consumer.[43] This provision takes on importance when one considers how hard it could be for the consumer to track down a suspected error by herself. Further, without this provision an error could result in the freezing of some or all of a consumer's assets.

III. Stored Value Cards

{15}"Stored value card" is really a functional description for a few different technologies where the card is a proxy for the exchange of hard currency for services or goods. It is different from checks, credit cards, and most other forms of proxy payments in that the value is transferred at the time of the transaction. Thus, it is more closely related to "check cards" or debit cards that deduct money from the user's account at the time of a transaction. The main difference between stored value cards and debit cards is commonly held to be that the former contain the value on the card itself, while the latter only point to the proper remote account for immediate value deduction. We will see that this is not always the case. Some stored value systems such as prepaid telephone cards rely on remote accounts that serve as short term, single purpose bank accounts.

{16}The main problem with stored value cards that make them a perfect target for fraud is that the user can neither directly "see" what is on the card nor what transactions have modified its contents. In a cash transaction, the consumer can count her change and dispute the transaction on the spot if necessary with physical proof . In an stored value card transaction, the consumer must rely upon either her own reader and display, or one provided by the other party, to verify what has been done to the data on the card. If there is no reader available, the consumer has no idea whether the correct amount was deducted--it is a "black box" transaction. Currently, the two main technologies utilized are magnetic stripe and integrated circuit cards.

A. *Magnetic Stripe Cards*

{17} Based on the same recording technology as floppy disks and audio tapes, magnetic stripe (mag stripe) cards retain up to one kilobit of data.[44] They are characterized by the black stripe--magnetic material combined with paint or binder--stamped or laminated onto one side which can be "swiped" through an electronic reader. Basically, this strip of material contains tiny magnetic particles that can be reoriented independently of each other. When the strip is passed over an electro-magnetic device (write head) the particles are polarized into patterns. When it is subsequently passed over a similar electromagnetic device (read head), the pattern is translated back into an electronic signal.

{18} Unfortunately, this system requires that the strip be exposed for access, resulting in vulnerability to physical damage and improper access. Further, the magnetic particles are susceptible to distortion from nearby magnetic fields, and can only be "rewritten" a limited number of times. On the other hand, a benefit is that the mechanism is cheap and has already been implemented in the extensive network of ATM and POS terminals across the globe. Thus, new mag stripe applications can be rapidly assimilated into a global network.

B. *Chip Cards*

{19} Advances in semiconductor technology have resulted in computer chips small enough to be embedded into credit card sized plastic housings, known as integrated circuits (ICs). [45] These chips are essentially electronic circuits--transistors and all--condensed onto one small piece of semiconductor material.[46] Three types of combined ICs power three types of cards: memory cards, challenge/response cards, and microprocessor cards.

{20} Memory chips allow data to be stored and retrieved so that cards containing them can have value loaded and deducted by anyone with the proper reader.[47] But, if the card is misplaced or stolen, anyone can use it. Likewise, a party contemplating accepting the card must have some means to determine whether the value stored is "genuine." We will consider these issues further in the section, "*Logistics and Economics of Stored Value Cards*" below.[48]

{21} Because memory chips offer no security for data, they are often installed with a "gatekeeper" logic chip that administers a "challenge/response" authentication feature that requires a personal identification number (PIN) to access the card's data.[49] Challenge/response cards can be configured both to protect the card's value in the event of loss or theft and to prevent an unscrupulous bearer from "reloading" value without actually paying for it.

{22} The addition of a microprocessor chip to make a "smart card" enables sophisticated authentication features, file systems, and actual data processing. Existing smart cards generally employ an 8 bit processor running at 10 MHz.[50] As full-fledged processors, they can, theoretically, perform all the computing functions of a PC. Although, practically, minimal memory and lack of interface or peripherals precludes such extensive applications. Yet a card that can perform its own complex data processing, account calculations and sophisticated identification verification[51] is attractive to a wide consortium of commercial and government organizations.[52] The inclusion of a stored value function is a low cost and profitable value-added feature.

C. *Logistics and Economics of Stored Value Cards*

{23} The various technologies employed for stored value cards result in different operational and economic consequences. An important conceptual distinction is "closed" vs. "open" systems. Closed systems are exemplified by many subway systems: riders deposit cash in the system's ticket dispensing machines which, in turn, produce tickets that can only be used in that system. Open systems are exemplified by some university systems: students purchase cards that can be used in transactions with unrelated vendors on, and sometimes off, campus.

{24} Closed systems present fewer challenges to potential card issuers and redeemers because there are no third parties involved. Since the same organization issues and redeems the card, there is little incentive for fraudulent misrepresentation of transactions between the issuing entity and the redeeming entity. Further, closed system operators can better monitor their cards for consumer fraud through direct control and familiarity. Thus, closed systems can be adequately managed with mag stripe cards, and the cost of entering a market with this type of system is relatively low. Perhaps because of all this, closed systems have already been deployed while open systems are still in testing.

{25} Presently, closed mag stripe card programs are used in the subway systems of San Francisco and Washington, D.C. They are also employed as prepaid phone cards.[53] The success of these programs, combined with all the recent attention given to electronic commerce, has led financial institutions and other organizations to investigate open stored value systems.[54] Chip cards can replace cash with "electronic" or "digital" cash that can be used with third party vendors who choose to accept it. The hook for issuers is the incredible amount of "float" possible from the aggregate of millions of cards, each loaded with value that may not be redeemed for a month or more.[55] Further, it targets the enormous, untapped small cash transaction market (less than $20) that is estimated at $750 billion to $2 trillion annually.[56]

{26} Mag stripe cards will probably not be used for open systems because the small value exchanged in the targeted transactions could be swamped by the necessary online verification costs. Also, a substantial portion of the market potential exists in places inhospitable to telecommunications links. Thus, financial institutions such as Visa are turning to chip cards because of their greater versatility and security.[57] It is also notable that the financial institutions are testing full microprocessor cards--"smart cards"--that will contain all of the bearer's financial records. Visa has dubbed these "relationship cards."[58] Ultimately, stored value will be only one of many applications housed on the card; others might be credit/debit, mortgages, and loans.[59]

{27} Non-banking organizations are also poised to enter the small transaction stored value card market, similar to the rush to provide prepaid phone cards.[60] There is already significant fraud, however, perpetrated in two directions: against issuers and against consumers. Three types of fraud against issuers are counterfeiting, skimming, and buffering.[61] While there are some ways to counter these frauds, they can be costly and imperfect.[62] On the other hand, many of the closed systems appear to be relatively successful, despite these problems.

{28} Fraud against consumers is the main focus of this paper, though, and the rapid proliferation of prepaid phone cards is instructive as to the type and magnitude of consumer fraud that unregulated stored value systems are vulnerable to. Rising from use by only 1% of U.S. households in 1995 to 10% in 1996, phone cards are now a $1 billion annual business.[63] But at the same time, many card issuers have failed and left consumers with worthless cards.[64] Further, because there are no regulations such as disclosure requirements, many cards have hidden fees and surcharges, while others expire after a fixed period whether the calling time has been used or not, and some simply never work.[65] Perhaps more concerning, though, the prepaid phone card business has become attractive enough that even the Mafia is reported by the New York Times to be moving quickly into it as a means to make up for the curtailment of some of its core businesses.[66]

{29} None of this bodes well for the rollout of general purpose open stored value systems from the consumer's perspective. Because the potential market for these generic cash alternatives dwarfs the single specific prepaid

phone card market, the incentive for fraud on unwary consumers will be almost irresistible. Even the nation's bankers are concerned about the creation of a chaotic alternative currency system that will coexist alongside the established federal currency system.[67] Thus, by providing a regulatory loophole that allows businesses to avoid regulation without substantially modifying their plans, the proposed *de minimis* exemption will be an open invitation to fraud.

IV. The Proposed De Minimis Exemption To Regulation E

{30} In 1994, Reg E underwent a routine review in accordance with the Federal Reserve Board's Regulatory Planning and Review program.[68] The final revisions to existing provisions were announced on April 23, 1996.[69] But this review also sparked debate over how stored value cards should be treated under Reg E. Are their contents "accounts" as defined by the rule? Is their use an EFT within the congressional intent embodied in EFTA? Or, within the rule as it exists now? Thus, on April 3, 1996, just before releasing the final rule on the 1994 revisions, the Board issued a Request For Comments on a proposed amendment to Reg E specifically encompassing stored value cards.[70]

{31} The proposed amendment would add a new section--205.16-- to Reg E specifically for stored value services.[71] While the new section appears to impose modified Reg E provisions on different types of stored value cards, the *de minimis* exemption buried in each covered category eviscerates any practical regulatory impact. The Federal Reserve Board treats low value (less than $100) stored value cards as a mere subset of the entire stored value market, but there is ample evidence that such cards will comprise the overwhelming bulk of the market.[72]

A. *The Proposed Amendment's Categorization of Stored Value Systems*

{32} The Federal Reserve Board distinguishes three categories of stored value systems. A brief assessment of the Board's incomplete understanding of stored value mechanics may help shed light on the problematic *de minimis* exemption, as well as set the stage for a better solution proposed at the end of this paper. Essentially, a two variable matrix consisting of an "online/offline" and "accountable/unaccountable" distinction is created. The first category, "off-line accountable stored value systems," is defined as programs where "the balance of funds available is recorded on the card, but is also maintained at a central data facility at a bank or elsewhere."[73] This type of program is probably exemplified by closed university systems where students deposit money in a school bank account and receive a fixed value card redeemable at retail outlets around campus. The Board deems these sufficiently similar to standard deposit accounts to fall under Reg E provisions.[74]

{33} The next category, "off-line unaccountable stored-value systems," are systems where "the record of value is maintained only on the card itself."[75] The Board asserts that "[g]iven the lack of a centrally maintained, ongoing record of individual card balances or of transaction data in these systems, it is more difficult to conclude that an 'account' exists for purposes of Regulation E."[76] These two categories are supposed to exhaust offline stored value programs, yet they omit an important offline variation: smart stored value cards that retain long-term, detailed transaction and account records. As in the example of Visa Cash above,[77] financial institutions are looking towards microprocessor cards that can retain all of a consumer's financial data. These records will be as valid and "permanent" as the bank's own records.[78] Thus, a third hybrid card category exists that is "accountable" in the Board's parlance without the need for an external data facility.

{34} For online systems, only one category is given without any distinction between accountable and unaccountable. Instead, all online systems are "the functional equivalent of using a debit card to access a traditional deposit account," and "involve[] on-line access to a database for purposes of transaction authorization and data capture."[79] This may not be a correct assessment of possible systems, however. Some prepaid phone cards that store value in a remote account and require an online connection may maintain transaction records while others may not. Thus some will be "accountable" in the Board's terminology, while other will not be.

{35} Finally, the Board offers a questionable distinction between online stored value systems and debit systems when it notes that "the value associated with a [stored value] card is limited to the amount that the cardholder has chosen to make accessible through the card (as opposed to a deposit account accessed by debit card, where the entire account is accessible and funds available may fluctuate)."[80] In one regard this is true of any EFT card: Cardholders choose how much value to associate with the card when they decide how much money to deposit in the accessed account. Further, in virtually all EFT-accessible accounts, the "entire account" is accessible.[81]

B. *The* De Minimis *Exemption and its Consequences*

{36} In the Comments accompanying the proposed amendment, the Board considers the impact of imposing existing Reg E provisions on each category and expends the bulk of its effort outlining modified Reg E coverage that appears to extend at least some consumer protections for most categories. Yet, it consistently eviscerates such protection by either exempting the category from Reg E coverage altogether or by including a $100 *de minimis* exemption into categories over which coverage is ostensibly being extended.

{37} More specifically, off-line accountable and on-line stored value systems are subject to a *de minimis* exemption of cards capable of storing only up to $100,[82] while off-line unaccountable stored value systems are purposefully not addressed in the proposed amendment.[83] In the Comments accompanying the proposed amendment, the Board justifies the *de minimis* exemption by simply stating that, "[f]or a stored-value product limited to a relatively small amount of funds, the amount at risk would be sufficiently minimal that application of even modified Regulation E protections appears unnecessary."[84] Further, the Board appears to buy into the industry clamor that imposition of Reg E requirements such as transaction receipts will unduly burden the economic feasibility and development of the stored value card market: "[I]f transaction amounts are on average quite small (as is likely to be true if the maximum amount on a card is low), the cost impact of Regulation E compliance would be proportionately greater than for systems involving large transactions."[85]

{38} The Board seems less decisive about not extending any Reg E coverage to off-line unaccountable stored value systems. So long as off-line unaccountable systems involve only "small dollar amounts and a single use, such as paying transit fares"[86] the Board sees no problem in denying Reg E coverage, probably under a similar rationale to that given for the *de minimis* exemptions in the other system categories. On the other hand, where offline unaccountable systems involve "substantially larger transaction amounts and maximum card values, and could have multiple uses," then the Board will view these as "more comparable to traditional debit cards than the small-value cards."[87] As such, the Board would consider bringing such systems under a modified Reg E coverage similar to its proposal for off-line accountable systems.

{39} It is interesting that the Board acknowledges the possible overlap between debit systems and large offline unaccountable systems, while appearing to deny it with regards to off-line accountable and on-line stored value systems. But more importantly, all of this discussion is a bit of a red herring because even if off-line unaccountable systems are brought under the "protection" proposed for the other categories, it will still be subject to the same *de minimis* exemption.

{40} The impact of the *de minimis* exemption is what really matters, however. As was already mentioned, the major financial institutions who are advancing into the stored value market are almost exclusively interested in the less-than-$20 transaction arena. This is only a fraction of the $100 *de minimis* exemption cutoff and thus renders a $100 maximum card feasible. In fact, most subway and telephone cards currently have $20 maximums. Coupling this with a strong regulatory incentive for $100 maximum cards--i.e. complete absence of Reg E coverage--means that it is highly likely that card issuers will stick with $100 maximum card systems. In turn this will result in a strong probability that any given stored value card system will not be covered by Reg E.

{41} The following forgone consumer protections will result:

Initial disclosures. Even the Federal Reserve Board notes that in the absence of this protection, "consumers might regard off-line accountable stored-value products as comparable to debit or credit cards, and thus might expect similar rights and remedies to apply."[88]

{42}*Change in terms notice.* Despite the Board's view that stored value cards will not have an expected life long enough to make this protection an issue,[89] many stored value systems utilize durable, reloadable cards that could last a number of years.[90] Given this fact, it seems ludicrous that stored value card issuers could enact hidden fees, changes in function, or shifts of liability without notifying the card holder.

{43} *Transaction receipts and periodic statements.* While the Board asserts that, "for small or commonly-made transactions, many consumers may not want or need a receipt,"[91] this logic was hardly persuasive when Congress passed the EFTA in the first place. Neither has it moved the Board to rescind the receipt requirement from existing Reg E provisions. Likewise, although the Board offers that consumers "may not need or want documentation on a periodic statement,"[92] this has not exactly been persuasive in the development of Reg E to date. In fact, receipts are the most important regulatory bulwark against an influx of "black box" transactions where fraudulent vendors shave pennies off each transaction, or simply siphon off the entire value in one exchange. And while there may be some short term cards where periodic statements are moot, many issuers are looking at long term "relationship cards." Most consumers would not be comfortable with a bank account that did not issue periodic statements so that they could check for errors; neither should they have to accept long term stored value cards without periodic statements.

{44} *Error resolution procedures.* The Board acknowledges that "an error within the financial institution's control, such as one resulting from a malfunctioning card, may not be unduly difficult to correct."[93] Why deny consumers the important protection afforded by requiring error resolution procedures already in place? Failing to mandate error resolution procedures is likely to allow card issuers to hold consumers' funds hostage while proceeding at a snail's pace to resolve a contested transaction.

{45} Two other Reg E protections concerning liability and unsolicited issuance were omitted from the preceding list because they truly may not be as appropriate in the stored value card environment. First, limitations on consumer liability for unauthorized transfers will not work in the case of non-authenticating, offline stored value systems. These cards are just like cash in that anyone can use them without any form of authentication. Placing the burden of lost or stolen cards on issuers who can do nothing to prevent it is like requiring banks to pay customers who happen to get robbed while not on the bank's premises. However, for authentication cards, this blanket exemption is entirely inappropriate.

{46} Second, the restriction on unsolicited issuance of access devices is largely irrelevant for stored value cards because the consumer will not have been able to place any money on the card yet. Thus, this provision is only relevant where the issuer could somehow transfer some of the consumer's assets to a card without permission and then send the unsolicited card to the user. Clearly, the first step would be fraud in and of itself.

V. A Better Compromise

{47} This paper has argued that the rapid emergence of stored value cards and systems has brought with it enormous potential for fraud, and that the *de minimis* exemption buried in the proposed Reg E amendment allows issuers to tap into exactly the market they want with no regulation. By not imposing existing Reg E protections such as initial disclosure, transaction receipts, and error resolution procedures, the amendment opens the door for fraudulent issuers to disburse cards that do not really contain the paid-for amount, or that expire before the consumer has had a chance to use all the value stored. The lack of Reg E protection also enables unscrupulous vendors to shave off a few extra pennies (or more) on each transaction. Further,if the industry is allowed to continue in an unregulated fashion, these scams may be only the beginning,. Industry interests have claimed that regulation will kill this nascent, potentially useful technology before it has a chance to flourish and work out some of the "bugs." The last section of this paper outlines a Reg E amendment that achieves a better

balance between the competing values of encouraging the development of new financial tools while protecting consumer interests.

A. *Recategorization of Stored Value Systems*

{48} The first step in creating a better Reg E amendment is to eliminate the *de minimis* exemptions. The second is to establish a more complete taxonomy of stored value systems. There are five variables to consider: online/offline, accountable/unaccountable, open/closed system, disposable/reloadable, and anonymous/authenticated. These definitions need to be modified slightly from the Board's versions.

{49} "Online" encompasses every stored value product that requires an online connection for *any* reason to complete a transaction.[94] "Offline" accommodates everything else. "Accountable" systems retain detailed, protected records of transactions for an indefinite period of time.[95] "Unaccountable" systems comprise the rest. "Open" systems exist where the card issuer and redeemer are not the same. In "closed" systems, the issuer and redeemer are the same.[96] "Disposable" cards can be loaded only once, regardless of how much can be loaded in that first instance. "Reloadable" cards can have value loaded at least once more after the initial value is installed. Finally, "anonymous" systems lack user authentication during the transaction. "Authenticated" systems employ identity verification, but distinguish between "pseudonymous" and "actual" identification. "Pseudonymous" verification uses a PIN or other access code issued at the time of purchase to restrict usage to a person who has purchased the value on the card.[97] Knowledge of the code is sufficient identification for the transaction. "Actual" verification is where the card is issued to *a particular person*--i.e. the card is non-transferable--and identification at the time of transaction must be deemed sufficient to verify the identity of that particular person.[98]

B. *Suggested Modified Reg E Coverage of Stored Value Systems*

{50} The foregoing may seem complex, but actually generates only a few important combinations that can be placed into a hierarchical flow chart. For *all* stored value systems a few Reg E provisions should always apply. Knowledge of the code is sufficient identification for the transaction.

1. *Provisions Covering All Stored Value Systems*

{51} First, initial disclosures of some minimal kind must always be provided. They could be printed on the card, issued as an accompanying receipt, or prominently displayed at the point of sale. This requires little to no additional cost to the issuer, yet can have immense importance to consumers unfamiliar with the new systems. Second, some minimal error resolution procedures must be in place. Existing Reg E error resolution requirements already take into account the fact that some types of investigation may be hopeless or extremely burdensome. Stored value service providers are simply asked to take reasonable efforts to resolve consumer complaints--in some cases there may be simply no way to determine whether a card was defective for example. But, within the same system, there may be some problems that can reasonably be investigated. Third, displays at transaction terminals must be available. Without this provision, vendors may be encouraged to use "black box" terminals that prevent the consumer from monitoring transaction proceedings.[99]

{52} Taken together, these provisions guarantee a uniform baseline of consumer protection without unduly burdening the developing stored value service industry. Building off this baseline, particular additional requirements may apply to functional variations of stored value systems.

2. *Provisions Covering Closed Stored Value Systems*

{53} Although the Board largely overlooks the open/closed system distinction, it probably has the most impact on system design and function. As described above, closed systems are easier to implement because the same entity issues and redeems the card. Third party fraud incentives are eliminated. Further, the consumer has only one organization to deal with when problems arise. Thus, it may be acceptable to impose fewer restrictions on closed systems than on open systems. For all closed systems, transaction receipt requirements should be eliminated. Issuance of receipts in a true closed system may be redundant: It is a little like receiving a merchandise credit in a department store, and then being issued a receipt for every item you pick up. More importantly, the major fraud incentive generated in an open system between card issuers and redeemers is absent, so proof of each and every transaction is less important.[100]

{54} *Disposable Stored Value Cards.* Closed systems may employ disposable cards, reloadable cards, or both. In the case of disposable cards, other standard Reg E provisions may be modified. First, periodic statements are largely irrelevant. Where the disposable card is accountable, card histories[101] should be available upon demand. For unaccountable cards this is clearly impossible, so no form of periodic statement or card history is required.[102] Second, regardless of the accountable/unaccountable distinction, disposable card closed systems should be exempt from change in terms and annual error resolution procedure notices requirements. Consumers will probably not retain cards long enough for these protections to be relevant. It may be prudent to incorporate a limited grandfather clause which requires, absent notice, observation of the terms and conditions extant at the time of card issuance for the life of the card.[103]

{55} *Reloadable Stored Value Cards.* In the case of reloadable cards, the analysis is different. First, periodic statements are relevant. For accountable card systems, statements should be available upon demand. For unaccountable card systems this is, again, probably impossible.[104] Second, all reloadable card closed systems should make change in terms and annual error resolution procedure notices available upon demand, or posted conspicuously near system transaction terminals. Alternatively, cards could be electronically date stamped upon issuance and with each subsequent reload, the date-stamp can be compared with the effective date of any change in the cards' terms or conditions. If a change has occurred, the terminal either prompts the card holder to request the updated notices or prints them automatically.

3. *Provisions Covering Open Stored Value Systems*.

{56} Open systems must instill confidence in both issuers and redeemers that access devices are valid. At the same time, participating organizations have an incentive to "pass the buck" when consumers run into difficulties, because it is easy to blame an unrelated organization for the alleged error. Thus, it is unlikely that mag stripe technology will be able to support an open system. Instead, major open system initiatives such as Visa Cash have used chip cards--often full microprocessor cards--in anticipation of the rollout of "relationship cards".[105] Using chip cards requires two things. First, it is easy to configure these cards as accountable. In fact, they may have to be accountable to instill enough confidence among issuers and redeemers. Second, new terminals need to be installed to accommodate these cards. The existing debit/credit network terminals are based on mag stripe technology.

{57} Consequently, transaction receipts should not be unduly burdensome. Small terminals capable of issuing receipts and accepting everything from credit cards to cash have begun turning up at many gas stations. Thus, small printers cannot be prohibitively expensive. The standard industry argument that the cost of printing receipts may overwhelm the value of the transaction is virtually impossible at present. Even the smallest transaction involving standard US currency ($.01) represents far greater value than the cost of printing a small receipt with inexpensive ink/toner on thin paper.[106] Further, this argument has never precluded receipts upon demand for low value cash sales.

{58} *Disposable Cards.* Similar to closed systems, open systems should be categorized into disposable and reloadable variations. For disposable cards, the modified provisions are essentially the same.[107] Periodic

statements, change in terms notices, and annual error resolution procedure notices are all waived. For accountable cards, possibly the only kind for open systems, card histories should be provided upon demand. Where they exist, unaccountable cards will have no such requirement.

{59} *Reloadable Cards.* Reloadable cards should provide change in terms and annual error resolution procedure notices upon demand. But, in open systems, the alternative of posting notices in conspicuous locations within system facilities is essentially impossible. Issuers cannot reasonably be expected to post changes in every third party location where their cards might be accepted. Instead, cards should be electronically date stamped upon issuance and reload. This date is then compared at subsequent reloads with the effective date of any changes in the cards' terms and conditions. If a change has occurred, the terminal either prompts the card holder to request the appropriate notice, or prints the notice out on the spot. Where reloadable cards are accountable, periodic statements upon demand should be required. Unaccountable cards, if possible, would be exempt from this condition.

4. *Miscellaneous Provisions*

{60} Two final distinctions must be addressed. First, the Board distinguishes between its conception of online and offline systems by correctly noticing that online systems closely resemble traditional deposit accounts. But, the Board refrains from extending full Reg E coverage to them. Online systems that access remote accounts are simply disguised asset accounts, however, and should fall under standard Reg E coverage. A regular deposit account established solely for the purpose of making funds accessible is still deemed an asset account. If it can be accessed by an EFT access device, it falls under Reg E coverage.

{61} Second, the distinction between anonymous and authenticated systems needs to be clarified. Anonymous systems allow anyone to access the card and account. Authenticated systems use a PIN or access code to monitor access in two ways. "Pseudonymous" authentication allows the card and code to be freely transferable. "Actual" authentication restricts the card and account to a specific user. The implication of this is that Reg E limits on consumer liability for lost or stolen cards are valid only for online authenticated systems. As the Board observed, it would be nearly impossible for issuers to notify all potential offline terminals of a lost or stolen card, and unauthenticated systems do not establish card/account ownership.

VI. Conclusion

{62} The sole purpose of the EFTA and Reg E is to protect consumers in new and unfamiliar electronic financial applications that have the potential to defraud them of significant amounts of money. The Federal Reserve Board has failed to fulfill Congressional expectations in this regard by proposing an amendment to Reg E ostensibly extending consumer protections to stored value cards, but which in fact enables the industry to operate in an unregulated environment through the inclusion of a $100 *de minimis* exemption. At least, the problem with this proposal stems from the value of $100 to different groups of citizens. For some it is indeed a "trifling" matter, while for most others it is a substantial amount. This paper operates from the premise that consumers should not be put in the position of accepting the loss of $100 "here and there" at the hands of high-tech con men, just to encourage an already profitable industry. As such, a workable amendment to Reg E is outlined which does not include the *de minimis* exemption. This modified Reg E amendment strikes a better balance between consumer and industry interests consistent with the legislative intent of the EFTA.

---

[*] Sean O'Connor is an associate with Weil, Gotshal & Manges LLP. He earned his J.D. from Stanford Law School 1998 and was the 1996 Brown & Bain Fellow in Law & High Technology. The author would like to

thank Jack Brown for funding the Brown & Bain Fellowship from which the original research for this article derived, as well as Kent Walker and Ken Rosenblatt for comments on earlier drafts of this article.

[**] **NOTE:** All endnote citations in this article follow the conventions appropriate to the edition of THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION that was in effect at the time of publication. When citing to this article, please use the format required by the Seventeenth Edition of THE BLUEBOOK, provided below for your convenience.

Sean M. O'Connor, The *De Minimis* Exemption of Stored Value Cards From Regulation E: An Invitation to Fraud?, 5 RICH. J.L. & TECH. 6, (Winter, 1998), *at* http://www.richmond.edu/~jolt/v5i2/oconnor.html.

[1] Electronic Fund Transfers, 61 Fed. Reg. 19696, 19703 (1996) (to be codified at 12 C.F.R. pt. 205).

[2] Credit card type devices that already contain value, or provide access to a specific value account. Current common stored value cards are prepaid telephone calling cards, and reloadable subway cards.

[3] *See* 12 C.F.R. pt. 205.

[4] *See Experts Ask: What is the Value of Stored-Value*?, Bank Network News, February 11, 1997.

[5] *See* Colin Baptie and Nicola Adamson, *VISA Cash: The Next Frontier in Payment Processing* (visited October 14, 1998) <http://cardshow.com/applications/VisaCash/next_frontier.html>.

[6] Jeffrey D. Zbar, *Visa's New Smart Card Brew*, Credit Card Mgmt., June 1, 1997, at 80.

[7] Prepaid phone cards are currently offered by organizations from telecommunications corporations to local convenience stores, and generally are issued in amounts ranging from $5 to $20.

[8] Board of Governors of the Federal Reserve System, Final Rule: Electronic Funds Transfers, 12 C.F.R. pt. 205 (May 2, 1996).

[9] In fact, the Smart Card Forum--a trade association composed of many of the largest banks, telecommunications companies, and smart card manufacturers--has publicly supported the proposed amendment. *See* John L. Burke Jr., *The Smart Card Forum, Legal and Regulatory Implications of Advanced Card Programs* (paper delivered at the CardTech/SecurTech conference, May 16, 1996) (visited October 14, 1998) <http://www.smartcrd.com/info/more/legal.htm>.

[10] Dean Anason, *Nonregulatory Responses Urged for Stored-Value Cards*, The American Banker, July 18, 1997 at 2 (quoting Janet Koehler, Senior Manager, AT&T Universal Card Services).

[11] *Consumer Advocates Seek Smart Card Regulations*, Retail Delivery Sys. News, June 20, 1997 at __.

[12] *Id.* at ___ (quoting Judith Rinearson, Group Counsel, American Express, Stored Value Group).

[13] Telephone interview with John Burke, counsel to the Smart Card Forum.

[14] Michael N. Castle, *Electronic Money and Banking: What Should Government's Role Be?* USA Today (Magazine), May 1997 at 26.

[15] *See Consumer Advocates Seek Smart Card Regulations, supra* note 11 (citing Mark Budnitz, Professor of Law, Georgia State University, and Margot Suanders, Managing Attorney, National Consumer Law Center).

[16] *See* 15 U.S.C. §§1693-1693r (1978).

[17] The Regulatory Planning and Review (RPR) program encompasses four goals: "to clarify and simplify regulatory language; to amend regulations to reflect technological and other developments; to reduce undue

regulatory burden on the industry; and to delete obsolete provisions." Board of Governors of the Federal Reserve System, Final Rule: Electronic Funds Transfers, 12 C.F.R. pt. 205 (May 2, 1996).

[18] *See* 15 U.S.C. §§ 1693-1693r (1978).

[19] *See* 12 C.F.R. § 205.1(b)(1998).

[20] *See id.* Thus, the Board's intent to balance consumer and industry concerns is in neither the act nor the regulation. Instead, it stems from the Board's own Regulatory Planning and Review (RPR) program.

[21] *See* 15 U.S.C. § 1693b (1998).

[22] *See* 12 C.F.R. § 205.3(b) (1998).

[23] *See id.*

[24] *Id*. at § 205.5(b).

[25] *Id*. at § 205.6(b)(1).

[26] *Id*. at § 205.7.

[27] *Id*. at § 205.8(a)(1).

[28] *Id.* at § 205.8(b).

[29] *See* 12 C.F.R. § 205.9(a) (1998).

[30] *See id.* § 205.9(b).

[31] *See id*.

[32] *See id.* § 205.10(a).

[33] *See id*. § 205.10(c).

[34] *See id*. § 205.10(d).

[35] *See id*. § 205.10(e).

[36] *See id*. § 205.11(a).

[37] *See id*. § 205.11(b).

[38] *See id*. § 205.11(c).

[39] *See id*.

[40] *See id*.

[41] *See id.*

[42] *See id.*

[43] *See id.* § 205.11(d).

[44] The equivalent of 226 alphanumeric characters. *See* Systems Resources Corporation, *Magnetic Stripe Card Technology* (visited October 14, 1997) <http://www.aitworld.com/techvalley/magstripe.html>.

[45] *See* The Smart Card Forum (visited October 1, 1998) <http://www.smartcrd.com>; Systems Resources Corporation, *Smart Cards* (visited October 14, 1997)

<http://www.aitworld.com/techvalley/smartcrd.html>.

[46] *See* M. Morris Mano, Digital Logic and Computer Design 30-31 (1979).

[47] Presently costing about $300. The Smart Card Forum (visited October 1, 1998) <http://www.smartcrd.com>.

[48] § II(C).

[49] Logic chip challenge/response capabilities are fairly limited, however, in that they can only handle simple codes and not sophisticated authentication features such as biometrics. Further, in the case of some proposed multi-application cards, logic chip security algorithms may not provide the desired variable protection for different directories--sort of an "all or nothing" problem.

[50] *See TB Family* (visited Oct. 7, 1998) < http://www.cp8.bull.net/prod/tbfam.htm>. By comparison, Pentium chips utilize a 32 bit processor running anywhere from 100 to 200 MHz.

[51] Such as biometrics where a user need only place a finger on an accompanying reader to generate an electronic fingerprint that is in turn fed into the card which matches it with the stored authentic user's print.

[52] *Id.*

[53] Most of the prepaid telephone card programs, however, are really debit systems where the value does not reside on the card but in an account maintained by the issuer.

[54] *See Hot Lines*, CardFAX, (Apr. 21, 1997) (discussing Citibank's VisaCash test in New York City); Colin Baptie and Nicola Adamson, *VISA Cash: The Next Frontier in Payment Processing* (visited Oct. 14, 1997) <http://www.cardshow.com/applications/VisaCash/contents.html>.

[55] Singapore's new CashCard has an estimated $10 billion float potential for banks, representing almost 10% of the total deposit base of all the island's banks combined. Alvin Tay, *Banks get new source of cheap funds*, The Straits Times (Singapore), Dec. 2, 1996, at 44.

[56] *See Experts Ask: What is the Value of Stored Value?*, Bank Network News, February 11, 1997., at 3; Colin Baptie and Nicola Adamson, *VISA Cash: The Next Frontier in Payment Processing* (visited Oct. 14, 1997) <http://www.cardshow.com/applications/VisaCash/contents.html>.

[57] *See* Colin Baptie and Nicola Adamson, *VISA Cash: The Next Frontier in Payment Processing* (visited Oct. 14, 1997) <http://www.cardshow.com/applications/VisaCash/contents.html>.

[58] *See id.*

[59] *See id.*

[60] *See* Steve Rosenbush, *More Players Deal Prepaid Phone Cards GTE, Texaco Issue Cards Featuring Missing Children*, USA Today, April 16, 1997, at B1.

[61] Counterfeiting produces unauthorized cards; skimming is fraudulent reloading of value; and buffering involves unauthorized manipulations of existing data. *See* Systems Resources Corporation, *Magnetic Stripe Card Technology* (visited Oct. 14, 1997) <http://www.aitworld.com/techvalley/magstripe.html>.

[62] *See Id.*

[63] *Prepaid Phone Card Prices Plummeting ; Per-Minute Charges Falling As More Firms Offer Service*, The San Francisco Examiner, February 26, 1997, at B-1 (citing International Telecard Association figures).

[64] Because these cards are unregulated, they are not insured by the FDIC (Federal Depositors Insurance Corporation). Some major issuers such as USA Calling, TLC-The Long Distance Co., and International Global Net have run into financial problems in the last few months leaving consumers with valueless unused time on their cards. *Id.*

[65] Anyone can get cards made cheaply enough and buy time from telephone companies, often on credit, to set up shop quickly and inexpensively. In the absence of any federal regulation, fly-by-night con-artists have become problematic enough to spur individual states such as Florida to consider regulating these prepaid phone card businesses themselves. *Id. See also* Jim Szymanski, *Prepaid Phone Cards Are Tempting Territory For Fraud*, News Tribune, February 02, 1997, at G1.

[66] Federal agents reported that the Gambino family defrauded consumers and telephone companies out of $50 million in New York and New Jersey alone by selling $20 cards that became worthless after only $2-3 had been used. Selwyn Raab, *Officials Say Mob Is Shifting Crimes To New Industries*, The New York Times, February 10, 1997, at A1.

[67] Of course, this may be mainly a case of protecting self-interest for the bankers, nonetheless the concerns are real for consumers as well. *See* Joseph Radigan, *Locking Up The Money Monopoly*, U.S. Banker, Jan. 1997 at 26.

[68] *See supra* at note 5.

[69] *Id.*

[70] Board of Governors of the Federal Reserve System, Proposed Rule: Electronic Fund Transfers (Regulation E; Docket No. R-0919) (April 3, 1996).

[71] *Id.* at 20-22.

[72] *See See Experts Ask: What is the Value of Stored Value?*, Bank Network News, February 11, 1997; Colin Baptie and Nicola Adamson, *VISA Cash: The Next Frontier in Payment Processing* (visited Oct. 14, 1997) <http://www.cardshow.com/applications/VisaCash/contents.html>.

[73] Board of Governors, supra, note 44 at 8. The Board does not mention that a single card must be the only means of access to the account, else a withdrawal or other deduction in the central account could occur while the presented card still indicates value in the account. This is given as a condition of online stored value systems**,** however.

[74] Board of Governors, at 8.

[75] *See id.*

[76] *See id.*

[77] Colin Baptie and Nicola Adamson, *VISA Cash: The Next Frontier in Payment Processing* (visited Oct. 14, 1997) <http://www.cardshow.com/applications/VisaCash/contents.html>.

[78] This is part of a larger trend towards "distributed" computing and record-keeping. Rather than overwhelm a central facility with data and computing tasks, local systems such as PCs or branch office file servers can perform many of these functions. Smart cards are an integral part of this development.

[79] *Id.* at 9.

[80] *See id.*

[81] One exception is when the account is structured in such a way as to preclude one owner from withdrawing all or some of the assets; then, the EFT card cannot access the entire account.

[82] Board of Governors at 20-21 (The *de minimis* exemption will be incorporated into the CFR as § 205.16(c)).

[83] *Id.* at 14 ("Under the proposed amendments, off-line unaccountable stored-value systems would not be covered by Regulation E. The proposed amendments do not provide an explicit exemption; instead, the definitions of systems that would be covered under the proposal do not capture off-line unaccountale systems.").

[84] *Id.* at 13.

[85] *Id.* at 17.

[86] *Id.* at 14.

[87] *See id.*

[88] Board of Governors, at 10.

[89] *Id.*, at 11.

[90] In fact, there is every reason to expect them to last as long as other bank cards currently do. The next generation of "smart" chip cards should last even longer as their contents are protected from the elements.

[91] Board of Governors, at 12.

[92] *Id.*, at 12.

[93] *See id.*

[94] The online connection may be simply for some form of user authentication: Not necessarily that the user is "John Jones," but that the user has the correct PIN and is the same person who purchased the card.

[95] A record that is kept only for the day or even week does not qualify.

[96] In the university examples, a card redeemable only at university-owned facilities is part of a closed system, while cards redeemable at non-university-owned facilities are part of an open system. Whether facilities are physically on or off campus is irrelevant for this distinction.

[97] This does not have to be the "original" purchaser--i.e. the person who bought the card from the issuer. Instead, this system allows transfer of the card and the code to any third party whom the original purchaser chooses.

[98] This could still be a PIN, but is increasingly likely to be a PIN plus photo ID/signature. Of course, a major facilitator of the coming stored value card/e-cash/digital commerce revolution is the digital biometric identifier which promises near-instantaneous verification of identification by testing a finger, hand, eye, or face placed near a small reader. With smart cards, the authentication can be done on the card, in conjunction with an on-site reader.

[99] This does not prevent fraud--an unscrupulous vendor could still misrepresent the transaction amount, but it both allows consumers to catch legitimate errors in the transaction and helps maintain honesty. Consumers will

soon be able to purchase "electronic purses" that allow access to the contents of some stored value cards, but this should not preclude protection for those that cannot, or who simply choose not to.

[100] We might consider requiring receipts for purchases of the initial card, or subsequent reloading.

[101] Documenting whatever information was recorded during each transaction.

[102] This may encourage system designers to utilize only unaccountable systems. However, other considerations regarding general system accounting can have a counterbalancing effect here.

[103] This could be accomplished by recording a simple date stamp in the card's data storage area. This could be done with little difficulty by mag stripe. Further, a fixed time limit, say one year, would override the grandfather clause.

[104] By definition, where the card, a mandatory online database link, or vendors compile data sufficient to identify the transactions later, the system has changed from unaccountable to accountable.

[105] Colin Baptie and Nicola Adamson, *VISA Cash: The Next Frontier in Payment Processing* (visited Oct. 14, 1997) <http://www.cardshow.com/applications/VisaCash/contents.html>.

[106] Proposed systems based on micropayments, transactions of a fraction of a cent, could validate the industry argument. However, if and when such systems become available, the Board will have to reconsider its position on Reg E and other financial regulations anyway.

[107] The only variation comes from the different overarching requirements for open versus closed systems.
