

Date: Dec 12, 2007

Proposal: Prohibition on Funding of Unlawful Internet Gambling

Document ID: R-1298

Document
Version: 1

Release Date: 10/01/2007

Name: Joe Samuel

Affiliation: First Data Corporation

Category of
Affiliation: Commercial

Address: 6200 South Quebec Street
Suite 270

City: Greenwood Village

State: CO

Country: UNITED STATES

Zip: 80111

PostalCode:

Comments:

December 12, 2007 Ms. Jennifer J. Johnson Secretary, Board of Governors of the Federal Reserve System 20th Street and Constitution Avenue, N.W. Washington, DC 20551 RE: Docket No. R-1298 Dear Ms. Johnson: On behalf of First Data Corporation, I am writing to provide our comments to the proposed rules by the Federal Reserve Board and the U.S. Treasury Department to implement applicable provisions of the Unlawful Internet Gambling Enforcement Act of 2006. We appreciate the opportunity to comment. By way of background, First Data is a U.S.-based technology services provider and a leading processor of electronic payment transactions. As a Fortune 500 company that employs approximately 29,000 employees globally and operates in 38 countries, our services help consumers, businesses and governmental entities make payments for goods and services using virtually any form of payment: credit card; debit and stored value card; electronic checks and paper checks at the point of sale; and over the Internet. We have a unique perspective with respect to the proposed regulations because our services enable the use and acceptance of electronic payments by way of our work with both financial institutions and merchants. Our merchant processing business facilitates merchants' ability to accept credit and debit cards by authorizing, capturing and settling their credit, debit, stored-value and loyalty card transactions at their physical locations, or over the Internet or at an ATM. We process over 30 billion payment transactions annually, including approximately half of all Visa and MasterCard credit and debit card transactions in the United States. A majority of these processing services are offered to merchants through joint ventures or similar alliance arrangements with financial institutions. Additionally, we own and operate the STAR network, one of the leading nationwide electronic funds transfer (EFT) networks, as well as the Instant Cash ATM network. Debit networks such as the STAR network provide a link between the merchant and the consumer's financial institution. We process personal

identification number (PIN)-based debit card and ATM transactions through these networks and perform other services for our financial institution customers. Generally, we support the agencies' approach with the proposed regulations in not proposing overly prescriptive regulations but providing covered entities flexibility in implementing processes and procedures designed to block restricted transactions. However, we have concerns with several areas of the regulations and offer the following comments as well as answers to some of the questions posed in the advance notice of proposed rulemaking. Comments on Specific Questions Raised in the Regulations. Background & Introduction Q: Is it reasonable that the final regulations take effect six months after the joint rules are published? A: No, we believe the final regulations should take effect no sooner than 12-18 months after the joint rules are published in the federal register for two primary reasons. First, we estimate that implementation of the proposed rules will take a minimum of 12 months due to the time required to enhance our payment processing systems. For example, while we employ a process to screen new merchants prior to establishing a processing contract, we will need time to alter this process since any merchant that would engage in illicit activity, such as unlawful Internet gambling, would not make this intention known to the processor by registering with the appropriate Merchant Category Code or otherwise. In fact, they would engage in this activity surreptitiously. Therefore, we would need more than the proposed six month timeline to modify and test our processes to facilitate adequate compliance with the proposed new regulations. Second, as the operator of the STAR EFT network, we believe that having an effective date of 12-18 months after being published in the federal register is necessary due to the time it will take all financial institution members of the network to adapt their systems to any new rules established by STAR to comply with the proposed regulations. Additionally, we ask that the actual effective date (in 12-18 months) be set so that it does not fall within the months of November to January due to internal system freezes. From November to January, merchant processors are running at peak system capability to accommodate the influx of electronic transactions occurring at retail merchants. Merchant customers prohibit their payment processors from performing enhancements or any type of internal system modifications that may impede the flow of their transactions. §A - Definitions. Q: Are any of the defined terms in the proposed regulation not sufficiently understood or defined? A: The definitions of "terminal operator" and "financial transaction provider" need to be refined to clearly specify whether payment processors are intended to be covered by these terms. For example, it is unclear whether acquirer processors are intended to be covered by the Act and/or the proposed regulations. Under the Visa/MasterCard Association rules, a merchant choosing to accept these branded cards as forms of payment from consumers must be "sponsored" into these associations by a member bank (e.g. acquiring bank). In other words, any one of the 2,000 banks in the United States that is a member of the card associations must be a party to the merchant processing contract. For the actual processing services, however, many bank members outsource to third parties like First Data. Although the regulations appear to point to the credit and debit card networks, associations and financial institutions, it is not clear how acquirer processors are to be treated. Separately, the definition of "bet or wager" appears vague. For instance, would an activity such as horse racing be considered a "sporting event?" Would "bet or wager" include a bet that is placed over the Internet but the actual payment occurs off-line or would "bet or wager" include a bet that is placed off-line but the actual payment occurs over the Internet? Does "bet or wager" include the placing of the bet or the payment or the payout? Would

paying a flat rate amount or a monthly subscription fee constitute a “staking or risking... something of value upon the outcome...” and therefore be considered a “bet or wager”? Such a clarification is necessary in that, according to the Act, the term "bet or wager" does not include, among other things, participation in any game or contest in which participants do not state or risk anything of value other than personal efforts of the participants in playing or points or credits that the sponsor provided free of charge and that can only be redeemed for participation in games or contests offered by the sponsor. Moreover, the proposed rule defers to other laws to define the very activity it seeks to prevent. In addition to the need for clarity in the definitions described above, it would be of particular value for the rule to expressly define what does and does not constitute unlawful Internet gambling. To leave this critical term defined only indirectly would require all entities subject to the proposed rule to aggregate a substantial volume of complex state and federal laws, which if even one is overlooked could cause the subject entity to violate the proposed rule. We strongly urge the agencies to carefully consider and clarify these points to reduce confusion and unintended non-compliance.

§B6 - Designated Payment Systems / Other Payment Systems. In the proposed regulations, ACH systems, card systems (including credit, debit and prepaid cards or stored value products), check collection systems, money transmitting businesses and wire transfer systems have been designated as systems used by a financial transaction provider that could be used in connection with or to facilitate a restricted transaction. Q: Is this list too broad or too narrow? Specifically, are there non-traditional or emerging payment systems not represented in the list that could be used in connection with or to facilitate a restricted transaction? A: First Data does not believe that the list can be narrowed due to the continuous emergence of new payment vehicles that would necessitate additional tracking or regulation.

§D - Processing of Restricted Transactions Prohibited. Comments were requested regarding the agencies’ approach that the Act does not provide them with the authority to require designated payment systems or participants in these systems to process any gambling transactions, including those transactions excluded from the Act’s definition of unlawful Internet gambling, if a system or participant decides for business reasons not to process such transactions. While the intent of the proposed regulations may be to prevent the over-blocking of transactions, we urge the agencies to strengthen the safe harbor provision by incorporating language clearly providing for liability protection if the blocking of a transaction (later deemed to be unreasonable) is done in good faith. In addition, we recommend that the agencies amend the regulations to provide unambiguous immunity from liability if the provider allows the transaction to proceed if it believes in good faith that the merchant’s actions did not violate the Act. To be clear, we urge the adoption of language that creates a more robust safe harbor for entities that have employed reasonable procedures to detect and prevent restricted transactions. Such a safe harbor provision should also provide immunity from actions brought by federal and state governmental entities for those providers that can show they have reasonable procedures in place to detect and deter restricted transactions.

§E - Reasonably Designed Policies and Procedures Comments were requested on the following examples of policies and procedures reasonably designed to prevent or prohibit restricted transactions: §E1 - Due diligence Q: Is it appropriate to incorporate due diligence procedures into account opening procedures? To what extent should the due diligence methods explicitly include periodic confirmation by the participants of the nature of their customers’ business? A: We have no objection to a general requirement for reasonable due diligence procedures to be incorporated into account opening

procedures. However, we strongly urge the agencies to not prescribe specific measures but rather provide non-exclusive examples of reasonable procedures. §E2 - Remedial action Q: Are the examples of remedial actions appropriate? Should additional examples be included?

A: Yes, we believe these examples are appropriate. However, in our view account termination would likely be the most realistic of the proposed actions. §E3 - Monitoring Q: Should ongoing monitoring and testing be included within the examples for the ACH, check collection and wire transfer systems? If so, how could this functionality be incorporated into the systems? A: We believe strongly that non-exempt participants in card systems should be given maximum flexibility to design and implement monitoring and testing procedures to detect possible restricted transactions. The covered entity should maintain sole discretion in determining how it will monitor and protect its system and trademark from unauthorized use.

Therefore, we urge the agencies to modify the proposed rules to clearly reflect that the examples provided are non-exclusive. Currently, the payment systems' policies and rules mandate that acquirers must perform certain monitoring functions. For example, merchant transaction deposits and submissions are continually tracked to identify changes in deposit or submission patterns that may indicate suspicious activity or to identify merchants who are possibly engaged in businesses differing from those indicated in their payment card acceptance contracts. §E4 - Coding Q: Should the procedural examples for the other designated payment systems encompass identifying and blocking restricted transactions as they are being processed? If so, how could such functionality be reasonably incorporated into the systems? A: Businesses that are engaged in illegal activity would not be inclined to code the transactions in a manner that would make them easy to identify and block. In reality, if an illegal Internet gambling code were to be established, it is highly unlikely that merchants would use it so that we, as a processor, could in turn block their transactions. Instead, it is our belief that the most effective ways to address this issue are to: (1) require contractual language prohibiting Internet gambling activity; (2) require due diligence at the time of relationship establishment; and (3) establish processes and procedures to investigate any allegations of improper activity. §E6 - List of Unlawful Internet Gambling Businesses Q: Is it appropriate for the agencies to establish and maintain this type of list and should examining or accessing the list be included in the examples of policies and procedures designed to block or prevent or prohibit restricted transactions? If it were practical to establish a list and a participant routinely checked the list, could the participant be deemed to have policies and procedures designed to prevent or prohibit restriction transactions if the participant took no other action? If a list were established and made available to all participants in the designated payment systems, should the exemptions be narrowed? Finally, would relying on such a list be an effective means of carrying out the purposes of the Act, even if unlawful Internet gambling businesses can change their corporate names with relative ease. A: We believe that establishing a list for known Internet gambling businesses could be helpful. However, in conjunction with such a list, we would strongly urge the agencies to create a safe harbor for payment system participants that can show regular use of the list. With that said, the agencies should be aware of the inherent challenges of creating this type of list, one of which is that businesses engaging in illegal activity could, and do, regularly change their names or otherwise disguise their identities and activities. As a result, the validity of such a list would undoubtedly be called into question. Conclusion We strongly urge the agencies to provide as much flexibility as possible for the payments system to comply with the proposed rules because various participants may find and employ differing and equally effective methods to

identify and prevent restricted transactions. In addition, we urge the agencies to establish an effective date that is a minimum of 12-18 months after the final rules are published. The payments industry needs time to establish new processes and procedures and to communicate with others in the payments stream, but to do so in six months would be all but impossible. In addition, we strongly urge the agencies to establish an effective date for the rules that falls outside of the November-January time frame to avoid disruption of merchant processing during the busy holiday season for merchants. Finally, we recommend that the agencies provide clearer definitions of “bet or wager,” “terminal operator” and “financial transaction provider” and “unlawful Internet gambling.” We appreciate the opportunity to comment on the jointly proposed rules by the Federal Reserve Board and the U.S. Treasury Department. Please feel free to contact me with any questions, comments, or concerns you may have. Sincerely, Joe Samuel Senior Vice President, Public Policy First Data Corporation (p) 303-967-7195 (e) joe.samuel@firstdata.com