

# ALL-IN: Internet

BY MICHAEL CARSON AND

THE FINAL RULE to implement the Unlawful Internet Gambling Enforcement Act (UIGEA) of 2006 is currently in effect, with a required compliance date of December 1, 2009, and it contains specific requirements for money transmitters, banks, and card system participants. In this article we will discuss the major provisions of UIGEA and how they apply to these payment systems. In addition, we will examine the response from the Federal Reserve and the Department of the Treasury to comments about the definition of unlawful Internet gambling and a potential “blacklist” of gambling Web sites, which received considerable attention from the payments industry.

## UIGEA Overview

As the name suggests, UIGEA seeks to curtail unlawful Internet gambling transactions (restricted transactions) by requiring payment systems to establish policies and procedures to identify and block or otherwise prevent or prohibit their customers from engaging in those transactions. The final rule implements these requirements and identifies the specific types of payment systems subject to UIGEA, which include automated clearinghouse systems, card systems, check collection systems, money transmitters, and wire transfer systems.



# Gambling Enforcement

ANDREW WIEDERHORN



Some participants in these payment systems are exempt from the requirements noted above that relate to restricted transactions depending on the nature of the relationship with the customer. For nonexempt payment system participants, the final rule provides examples of policies that can be used to comply with UIGEA's requirements. These policy examples focus on conducting due diligence at account signup to determine whether the customer engages in Internet gambling. Additional examples vary by payment system, and a more detailed discussion of some of those policies is included in the sections below.

Explanations for several key items in the final rule are also important to note, as they affect the scope of the requirements. The first, and most obvious, is the definition of unlawful Internet gambling. The final rule relies on existing state and federal law in defining this term, and the lack of guidance for payment systems on this issue was the subject of numerous comments to the proposed rule. We will later examine the agencies' reasoning for this approach.

Second, a safe harbor provision for "overblocking" transactions related to Internet gambling is contained in the final rule. This provision affirms that payment systems can continue to block transactions based upon internal business decisions even if those transactions do not fall under the definition of unlawful Internet gambling.

Last, the final rule clarifies that a payment system's policies regarding restricted transactions need apply only to commercial customer accounts.

## How the Rule Applies to Money Transmitters

While the final rule applies to money transmitters, a large number of them are exempt from its requirements. According to the agencies, money transmitters that do not allow remote fund transfers, such as through a Web site, are not likely to be used for Internet gambling. As such, all participants in a money transmitting business, including send agents, are exempt except for the operator of the business. The rule also specifically excludes check cashers, currency exchanges, and entities that issue or redeem money orders, travelers' checks, or similar instruments.

These exemptions added to the final rule represent a significant decrease in the number of money transmitters that are subject to its requirements. In fact, the agencies estimate that without the exemptions 253,208 money transmitters would have been affected by the proposed rule. The final rule's exemptions reduce that number to 16.



**The final rule implements these requirements and identifies the specific types of payment systems subject to UIGEA, which include automated clearinghouse systems, card systems, check collection systems, money transmitters, and wire transfer systems.**

There are various procedures nonexempt money transmitters can implement to address unlawful Internet gambling:

- Conduct due diligence for commercial customers at account opening to determine the likelihood they will engage in Internet gambling.
  - If a review of the customer's business indicates there is some risk it may conduct Internet gambling (for instance, if it offers games or contests), the money transmitter should request certification from the customer that it does not engage in Internet gambling. This certification should address factual questions regarding the business.
  - If a review of the customer's business indicates it does conduct Internet gambling, money transmitters should request the following to ensure the business is lawful: licensure by a regulatory body such as a state agency to operate an Internet gambling business or a legal opinion stating why the Internet gambling business does not involve restricted transactions; a written commitment from the customer to notify the money transmitter of any changes to the legal status of the business; and third-party certification that the customer's systems will remain within lawful limits.
- Notify customers through a user agreement or similar contract that restricted transactions associated with Internet gambling are prohibited.
- Conduct ongoing monitoring to detect potential restricted transactions associated with Internet gambling. This can include reviewing payment patterns to detect suspicious payment volumes to any recipient.
- Establish procedures to deny services or close accounts of commercial customers if the money transmitter has actual knowledge that a customer is involved with unlawful Internet gambling.

It should be noted that these are nonexclusive examples and the final rule allows for money transmitters to establish their own procedures in accordance with their business needs.

**How the Rule Applies to Banks and Card Systems**

The final rule implementing UIGEA includes special rules applicable to card systems requiring that certain transactions covered by UIGEA be coded, identified, and denied, blocked, or otherwise prevented. The agencies greatly reduced the burden associated with these special rules,

however, over the course of the UIGEA rulemaking, at least from the perspective of card system participants that are not system operators (e.g., merchant acquirers, payment processors, and card issuers).

For example, under the proposed rule, nonoperator card system participants faced a difficult choice—they could opt to either (1) avail themselves of the safe harbor provisions for entities relying on and complying with the written policies and procedures of the card system operator, but only to the extent these policies and procedures were reasonably designed to satisfy the requirements of the UIGEA rulemaking; or (2) establish and implement their own procedures reasonably designed to identify, block, and otherwise prevent or prohibit transactions restricted under UIGEA. Although the first option clearly was optimal for card system participants seeking to minimize cost and effort associated with designing a UIGEA compliance program, commenters criticized the cost, effort, and uncertainty that would have been associated with evaluating the adequacy of these policies and procedures under the UIGEA regulation, which made selecting this method of compliance a burdensome and potentially risky proposition. The perceived risks included the fact that neither UIGEA nor the proposed rule told card system participants how they were to determine whether the policies and procedures of the card system operator met the “reasonably designed” standard, which eliminated the certitude one might expect from a safe harbor. In addition, participants considering this option were left to wonder what ongoing monitoring obligations they had with respect to the card system operator's policies and procedures.

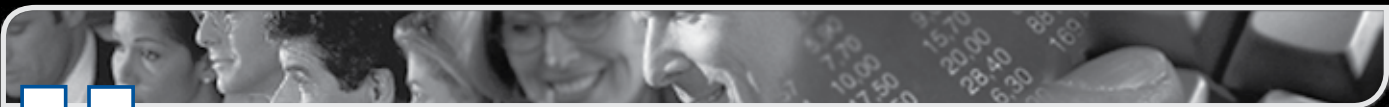
Alternatively, the compliance costs associated with the second option (implementing a standalone UIGEA compliance program) would have been fairly significant and could hardly have been achieved by any single card system participant. Any entity choosing this route would likely have had to rely on the card system operator for the merchant and transaction coding that the agencies clearly envisioned as underpinning transaction prevention efforts under the UIGEA. Such an entity would have been so dependent on the compliance design efforts of its card system operator that it would have had to wait for these efforts to be substantially completed before it could begin its own design efforts. This dependency would have caused the entity to lose partial control over its ability to implement UIGEA compliance efforts on time.

The final rule made the options available to nonoperator card system participants more palatable by vastly improving the UIGEA rule's reliance provisions. The agencies effectively "federalized" the analysis of the adequacy of any card system operator's policies and procedures and greatly clarified and simplified the procedural aspects of reliance. Under the final rule, in order to qualify for the reliance safe harbor, card system participants need only obtain a written statement or notice from the system operator indicating that it designed or structured the system's policies and procedures for identifying and blocking, preventing, prohibiting, etc., restricted transactions to comply with the requirements of the UIGEA rule. A participant can rely on such a representation by the operator until and unless the participant is notified otherwise by the operator or the operator's primary federal functional regulator or, if applicable, the Federal Trade Commission.

The final rule also significantly improved upon the monitoring elements of the proposed rule. Under the proposed rule, issuers, merchant acquirers, payment processors, and operators of card systems had to provide for ongoing monitoring and testing to detect transactions potentially covered by UIGEA in order to fit under a safe harbor. This would have included testing to determine whether appropriate coding for transaction authorization requests was taking place, monitoring Internet sites for unauthorized use of the relevant card system (including its trademark), and reviewing payment patterns for merchant customer accounts for suspicious volumes.

While the merits of requiring that each type of entity involved in a credit card system perform each of these tasks in order to qualify for the applicable safe harbor are debatable, the agencies effectively mooted this concern by revising their approach in the final rule. Under the final rule, entities involved in card systems can pick one of two approaches to complying with the final rule: (1) follow certain specified standards for due diligence on commercial accounts, which are very similar to the standards for money transmitters described earlier and are designed to ensure that the commercial accounts will not be used for prohibited Internet gambling activities; or (2) engage in transaction prevention based on transaction and merchant coding by the system operator. The final rule only makes monitoring a part of the transaction prevention approach to UIGEA compliance. It is expected that, among card system entities, only system operators will choose this compliance approach. By limiting UIGEA-related monitoring activities in this manner, the agencies essentially ensured that only the entities whose monitoring efforts one would expect to yield the best and most useful information (card system operators) would perform monitoring—a very sensible outcome.

The final rule also included a clarification of the due diligence requirement that no doubt was welcomed by the banking and money services business industries. The agencies noted that depository institutions with customers that are money transmitters are responsible for conducting due diligence only on depository institution customers. They



## Young & Associates, Inc.

BANKERS WORKING  
**FOR**  
BANKERS  
SINCE 1978

### Reg GG Tool Kit

Every bank involved in electronic banking channels will have responsibilities under Regulation GG and will be required to have policies and procedures in place by December 1, 2009.

- Payment Systems – ACH, Credit/Debit Cards, Checks, Wire Transfers, Money Transmitting Systems
- Exemptions
- Reliance on Payment Systems Policy and Procedures
- Risk-Rating Commercial Deposit Customers
- Due Diligence Requirements
- Certifications from Commercial Deposit Customers
- Third-Party Certifications
- Reasoned Legal Opinions
- Identifying/Blocking Transactions
- Requirement to Give Notice

#### Includes

- Policy
- ◆
- Training Manual
- ◆
- Compliance Monitoring Checklist

**800.525.9775**  
younginc.com

**For more information, contact Bryan Fetty at 1.800.525.9775 or product@younginc.com.**

are not responsible for assessing the risk that the money transmitting businesses' customers might engage in Internet gambling, a line of inquiry that would have resulted in a great deal of additional due diligence. Although an explicit statement by the agencies that an evaluation of the money transmitting business's due diligence policies and procedures under UIGEA is not required would have been ideal, one can easily infer this point from the fact that such a requirement is not present in the due diligence segments of the final rule's section setting forth examples of UIGEA-compliant policies and procedures. To their credit, it appears the agencies were very conscious of the perception that depository institutions incur increased compliance-related costs when they bank money services businesses and sought to prevent the UIGEA regulation from further fueling this perception.

### **Response to Comments on the Meaning of "Gambling" and Maintaining a List**

Prior to adoption of the final rule, the agencies solicited comments on the proposed rule first issued in October 2007. Two related topics that attracted a great deal of attention from commenters were the definition of unlawful Internet gambling and whether to establish a "blacklist" of operators of gambling Web sites.

As stated earlier, the final rule does not specifically define which gambling activities are illegal. In response to comments requesting more clarity around the definition of unlawful Internet gambling, the agencies said a single definition would not be practical because gambling laws vary at both the federal and state levels. They were also wary of interpreting gambling laws not under their jurisdiction. Instead, the agencies suggested due diligence steps (such as those detailed earlier) for use in evaluating potential commercial customers. Through this process, the stated intention of the final rule is to place the burden on commercial customers to prove they are not engaged in an illegal gambling business as opposed to having the payment systems make that determination on their own.

The agencies also sought specific comments on whether the final rule should include a "blacklist" of unlawful Internet gambling businesses. Under this concept, payment systems would utilize the list in determining which commercial entities enabled impermissible gambling under the UIGEA in order to identify the transactions that should be blocked. While the agencies received comments both supporting and opposing this proposal, they elected not to establish such a list, citing two main reasons: (1) the difficulty in interpreting the web of federal and state gambling laws that would be necessary to create the list; and (2) the challenges in maintaining an up-to-date list because of the ease with which businesses can change their names and payment information. In addition, the agencies suggested that the blacklist was unnecessary because the UIGEA already provides a course of action for government entities when they become aware of an unlawful Internet gambling Web site. The UIGEA provides for a procedure whereby certain state or federal officials may

institute proceedings to have these sites removed from the Web by the interactive computer service enabling Internet access to the site. Ultimately, the agencies apparently concluded that public policy considerations and industry's desire for certainty in complying with the final rule were better met by industry making use of the safe harbor provisions in the commercial due diligence segment of the final rule rather than by instituting a list-screening regime when the list itself might not be particularly current or accurate.

### **Conclusion**

As we detailed in this article, UIGEA and the final rule implementing the law affect a wide variety of payment systems. However, it is not a one-size-fits-all approach, and there are different requirements and exemptions based on a variety of factors, including the nature of the payment system's relationship to its customer and the likelihood that the payment system will be used for unlawful Internet gambling. In some cases, significant changes were made to the final rule based upon feedback from the payments industry. In other cases, the rule remained largely unchanged despite comments from various groups. While we provided a broad overview of these issues, payment systems should ensure they familiarize themselves with the specific requirements of the rule and its application to their business in advance of the December 1, 2009, compliance deadline. **BC**

### *ABOUT THE AUTHORS*

**Michael Carson** is the Manager of the North America Brand Risk Management Group in PayPal's Legal Department. He is responsible for developing and implementing policies to effectively manage PayPal's legal, industry, and brand risks. Prior to joining PayPal in 2005, Carson worked in the government relations field for an issues management group focusing on technology and privacy matters. In addition, he spent three years in the public sector serving as staff director for the Senate Minority Leader's Office in the Massachusetts State House. Carson is a Boston College graduate with a B.A. in Political Science. Reach him by telephone at (408) 967-4049 or via e-mail at [mcarson@paypal.com](mailto:mcarson@paypal.com).

**Andrew Wiederhorn**, who joined Capital One in 2006, serves as an assistant general counsel with responsibilities in the data security, internet gambling, fraud, anti-money laundering/Bank Secrecy Act, and OFAC areas. Prior to joining Capital One, Mr. Wiederhorn was an attorney with the Financial Services Practice Group of the law firm of Hogan & Hartson in Washington, D.C., focusing primarily on domestic financial services mergers/acquisitions and regulation. Mr. Wiederhorn began his legal career in the Domestic Banking Structure in the Federal Reserve Board's Office of General Counsel, where he held the titles of attorney and senior attorney. During law school, Mr. Wiederhorn was a summer law clerk at the Federal Reserve Board and the Office of the Comptroller of the Currency. He received his J.D. from Northwestern University and his undergraduate degree from Tufts University. Reach him via e-mail at [andrew.wiederhorn@capitalone.com](mailto:andrew.wiederhorn@capitalone.com) or by telephone at (804) 284 7701.