# Facilitating Financial Transactions in the Age of Internet Gambling: Compliance with the Unlawful Internet Gambling Enforcement Act

ANDREA L. MARCONI, GREGORY A. DAVIS, AND BRIAN M. McQUAID

*The authors discuss federal regulations requiring "designated payment systems, and all participants therein [to] identify and block or otherwise prevent or prohibit" the transmittal of funds knowingly accepted in connection with unlawful Internet gambling, and suggest due diligence policies and procedures that financial transaction providers should consider adopting.*

All but two states, Utah and Hawaii, permit some form of gambling.[1] While the gambling landscape had long been dominated by traditional brick-and-mortar casinos and state lotteries, the last decade has seen a tremendous growth in the Internet gambling industry. Today, nearly 15 percent of all gambling revenue is generated by the Internet gambling industry, and that percentage increases daily.[2] Indeed, in the last three years alone, the Internet gambling industry has increased its revenues by an estimated $1 billion per year.[3] While traditional domestic casinos and state lotteries gener-

Andrea L. Marconi, Gregory A. Davis, and Brian M. McQuaid are attorneys with Squire, Sanders & Dempsey L.L.P., practicing in the Phoenix, Arizona office. Ms. Marconi and Mr. Davis focus their practices on complex commercial litigation matters, including issues concerning the ACH Network and electronic payment transactions. Mr. McQuaid focuses his practice on complex commercial litigation matters. The authors can be reached at amarconi@ssd.com, gdavis@ssd.com, and bmcquaid@ssd.com, respectively.



Published in the July/August 2009 issue of The Banking Law Journal.

ate close to $85 billion in annual revenues, the Internet gambling industry now generates nearly $12 billion per year.[4]

In response to this incredible growth, the federal government passed sweeping regulations targeting the Internet gambling industry. Specifically, on October 13, 2006, President Bush signed into law the Safe Accountability for Every Port Act, otherwise known as the SAFE Port Act, which included as Title VIII the Unlawful Internet Gambling Enforcement Act of 2006 (the "UIGEA" or the "Act").[5] The UIGEA contains a comprehensive regulatory scheme designed at limiting the activity of persons and entities engaged either directly or indirectly in Internet gambling, including gambling website operators and the financial transaction providers or payment systems that facilitate Internet gambling transactions. Specifically, § 5363 of the UIGEA provides that it is a federal crime for any person or entity "engaged in the business of betting or wagering" to "knowingly accept" credit, electronic fund transfers ("EFTs"), checks, or other forms of financing as payment "in connection with the participation of another person in unlawful Internet gambling."[6] As such, financial transaction providers and payment systems who are merely engaged in the business of financing and payment processing are generally exempt from liability under § 5363.[7] Financial entities must, however, comply with § 5364 of the Act which requires "designated payment systems, and all participants therein" to "identify and block or otherwise prevent or prohibit" restricted Internet gambling transactions.[8]

Though the UIGEA premises criminality on a finding that an entity knowingly accepted payment in connection with "unlawful Internet gambling," the Act does not expressly define what constitutes "unlawful Internet gambling." The UIGEA, rather, relies on underlying federal and state law, and generally defines unlawful Internet gambling as knowingly transmitting a bet or wager that "is unlawful under any applicable Federal or State law in the State or Tribal lands in which the bet or wager is initiated, received, or otherwise made."[9] By defining unlawful Internet gambling in such a manner, the UIGEA requires entities to comply with a myriad of federal gambling laws including the Interstate Wire Wager Act ("Wire Act"),[10] the Interstate Foreign Travel or Transportation in Aid of Racketeering Enterprises Act ("Travel Act),[11] the Illegal Gambling Business Act ("IGBA"),[12] and the Racketeer Influenced and Corrupt Organizations Act ("RICO Act"), as well as gambling

laws in each of the 50 states.[13] Lawful Internet gambling activities, i.e., fantasy sports, state lotteries, horse racing and gambling on Native American lands, are exempted from the UIGEA's prohibitions.[14]

The substantial burden that compliance with the UIGEA imposes by virtue of its nonexistent definition of unlawful Internet gambling has been widely discussed by legal and industry commentators, and has even been acknowledged by the Board of Governors of the Federal Reserve System. Indeed, in her testimony to the House Subcommittee on Domestic and International Monetary Policy, Trade, and Technology, Louise L. Roseman, Director of the Division of Reserve Bank Operations for the Board of Governors of the Federal Reserve System stated: "The activities that are permissible under the various Federal and State gambling laws are not well-settled and can be subject to varying interpretations."[15]

On January 19, 2009, in accordance with the mandate of § 5364, which requires the Secretary of the Treasury and the Board of Governors of the Federal Reserve System to implement regulations requiring "designated payment systems, and all participants therein [to] identify and block or otherwise prevent or prohibit" the transmittal of funds knowingly accepted in connection with unlawful Internet gambling, the Secretary of the Treasury and the Board of Governors of the Federal Reserve System issued such regulations (the "Final Rules").[16] Compliance with the Final Rules is required by December 1, 2009.[17]

This article examines the contents of the recently-enacted Final Rules, including a discussion of which entities are required to comply with the Final Rules and those that are exempt from compliance, as well as the scope of the Final Rules' safe-harbor provision, which protects financial entities from liability for blocking restricted transactions as part of compliance with the Final Rules. This article then discusses recommended due diligence policies and procedures that financial transaction providers should consider implementing to comply with the Final Rules. This article also offers general suggestions for due diligence policies and procedures applicable to all financial transaction providers, regardless of the payment system the individual provider utilizes, and suggests unique procedures that are specific to each of the five payment systems identified in the Final Rules:

(1) the Automated Clearing House ("ACH") Network;

(2) the Credit/Debit/Stored Value Card system (the "Card System");

(3) the Check Collection System;

(4) the Wire Transfer System; and

(5) the Money Transmitting System.[18]

## CONTENTS OF THE FINAL RULES

### Exempt and Non-Exempt Participants

The Final Rules apply only to financial transaction providers that utilize one or more of the five designated payment systems identified in the Final Rules.[19] Within this group of financial transaction providers, however, the Final Rules exempt numerous participants from compliance.[20] Indeed, with the exception of the Card System, the Final Rules only require compliance by the participant that establishes and maintains a direct customer relationship with the Internet gambling business.[21] Therefore, as a general matter, if a financial transaction provider (unless a participant in the Card System) does not have a direct customer relationship with an Internet gambling business, the provider need not comply with the Final Rules.

For example, within the ACH Network, the Final Rules exempt all participants except: (1) the receiving depository financial institution ("RDFI"), and any third-party processor receiving the transaction on behalf of the receiver, in an ACH credit transaction; (2) the originating depository financial institution ("ODFI"), and any third-party processor initiating the transaction on behalf of the originator, in an ACH debit transaction; and (3) the receiving gateway operator and any third-party processor that receives instructions for an ACH debit transaction directly from a foreign sender.[22]

Within the Check Collection System, the Final Rules exempt all participants except the depository bank.[23] Similarly, within the Wire Transfer System, the Final Rules exempt all participants except the beneficiary's bank.[24] Lastly, within the Money Transmitting System, the Final Rules exempt all participants except the operator.[25] All other participants in each of the five

designated payment systems, including all participants in the Card System, an estimated 134,451 financial transaction providers in all,[26] are deemed non-exempt participants and must comply with the Final Rules by December 1, 2009.[27]

## Required Procedures

The Final Rules require all non-exempt participants in each of the five designated payment systems to establish, implement, and comply with "written policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit" the transaction of funds knowingly accepted by an Internet gambling business in connection with unlawful Internet gambling (a "Restricted Transaction").[28] Notably, the Final Rules merely require the non-exempt participant to "block" restricted transactions. As that term is defined in the Final Rules, the non-exempt participant need only reject a Restricted Transaction before or during processing and need not freeze the funds in question or otherwise prohibit all subsequent transfers or transactions regarding the proceeds or account.[29] As discussed in greater detail below, however, upon learning of a merchant customer's attempt to initiate a Restricted Transaction, a non-exempt participant must establish procedures specifying under what circumstances that merchant customer's account will be suspended or terminated.[30]

It is likely that the written policies required by the Final Rules must be reasonably designed to block Restricted Transactions by both new and existing merchant customers. Indeed, while many criticized the proposed final rules as being "unclear as to whether the due diligence requirement applies to both new and existing customer relationships," the Secretary of the Treasury and the Board of Governors of the Federal Reserve System adopted the Final Rules without adding the requested clarity.[31] Thus, the due diligence requirement is not likely limited to new merchant customers. Accordingly, financial transaction providers should also evaluate their portfolios of current merchant customers to monitor, identify and block Restricted Transactions from existing merchants.

If the operator of a designated payment system in which the particular financial transaction provider is a participant has "designed or structured the

system's policies and procedures for identifying and blocking or otherwise preventing or prohibiting restricted transactions," then a participant may comply with the Final Rules by implementing the policies and procedures set forth by its system operator rather than creating its own policies and procedures.[32] To date, however, no operator of a designated payment system has designed or implemented any policies or procedures to block Restricted Transactions. As such, for the time being, the onus remains on individual non-exempt participants to design and implement their own written policies and procedures to ensure compliance with the Final Rules.

## Safe-Harbor

The Final Rules contain a safe-harbor provision which shields a non-exempt participant from liability for blocking, preventing, or prohibiting the acceptance of its products or services in connection with a transaction, or otherwise refusing to honor a transaction if: (1) the transaction is a Restricted Transaction; (2) the non-exempt participant reasonably believes the transaction to be a Restricted Transaction; or (3) the non-exempt participant blocks the transaction in reliance of the written policies or procedures promulgated by the operator of the designated payment system in which the financial transaction provider is a participant.[33] Importantly, however, the safe-harbor provision does not protect a financial transaction provider from government liability for processing Restricted Transactions, even if unintentional.[34] For instance, the safe harbor provision does not protect a financial transaction provider from: (1) carrying out a transaction it learns to be restricted after the transaction is initiated, but prior to completion, or (2) inadvertently failing to block a Restricted Transaction despite complying with its written policies and procedures designed to identify and block such transactions.

With respect to the first scenario, liability may arise from completing a transaction and funding an Internet gambling merchant if the restricted nature of the transaction is discovered during processing (i.e. while the transaction is pending). In this situation, the Final Rules appear to imply that a financial transaction provider should return the transaction and refund payment to the original account. Indeed, in reference to the definition of the term "block," the federal government's comments to the Final Rules provide

that funds are not to be frozen, but rather are to either "remain in or be returned to the original account [to] be accessed by the accountholder for other purposes."[35] This suggests, therefore, that if a Restricted Transaction is discovered during processing the transaction is to be reversed and the funds returned to the original accountholder. Similarly, if a non-exempt participant funds a reserve or escrow account for its merchant customers by retaining a small percentage of the merchants' transactions, the non-exempt participant may face liability for distributing the reserve account to a merchant if the participant later learns that the merchant was initiating Restricted Transactions and, thus, that the reserve account was funded in whole, or in part, by Restricted Transactions. Such liability may, however, turn on the interpretation of the term "block." Under the Final Rules, "block" expressly does not require a participant to "prohibit subsequent transfers or transactions regarding the proceeds or account."[36] If this exception is interpreted to refer to the merchant customer's proceeds or account, then the term "block" may not require a participant to prohibit subsequent transfers of funds to merchant customers if the participant later learns the funds may include proceeds from Restricted Transactions. The availability of such an exception, however, likely presumes that the participant did not have knowledge at the time of processing the transaction that it was, in fact, a Restricted Transaction.

With respect to the second scenario in which the non-exempt participant does not learn of the nature of the Restricted Transaction until after all funds associated with the transaction have been transferred to the gambling merchant customer, no guidance can be found in the Final Rules. Thus, it is unclear whether a non-exempt participant may be liable for unwittingly processing a Restricted Transaction despite complying with its written policies and procedures to identify and block such transactions. In light of this uncertainty, and in order to establish a strong defensive posture to such potential claims, it is paramount that non-exempt participants design, implement and follow comprehensive policies and procedures to identify and block Restricted Transactions in order to rebut any allegation that they knew, or should have known, of the restricted nature of the transactions in question.

## RECOMMENDED PROCEDURES TO IDENTIFY AND BLOCK RESTRICTED TRANSACTIONS

### New Merchant Customers

#### *General Procedures Applicable to All Designated Payment Systems*

The Final Rules include non-exclusive examples of policies and procedures designed to identify and block Restricted Transactions.[37] Significantly, if a non-exempt participant implements the due diligence procedures contained in the non-exclusive examples in the Final Rules, such due diligence procedures "will be deemed to be reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions," and thus will satisfy the obligations imposed upon non-exempt participants by the Final Rules.[38]

To conform with the due diligence procedures set forth in the Final Rules, when establishing a new merchant customer account the non-exempt participant must conduct a due diligence review of the new merchant customer's business activities, and make a determination as to whether the new merchant customer "presents a minimal risk of engaging in an Internet gambling business," legal or otherwise.[39] The Final Rules provide that any agency, department, or division of a federal or state government, in addition to any entity that is directly supervised by a federal functional regulator, may be automatically deemed to present a minimal risk of engaging in an Internet gambling business.[40] Otherwise, however, the Final Rules leave it to the non-exempt participant's discretion to determine whether a new merchant customer only presents a minimal risk of engaging in an Internet gambling business and do not specifically define what constitutes "due diligence."[41] Accordingly, a non-exempt participant should consider implementing some or all of the following procedures, among others, as part of its process of examining and underwriting new merchant customers.

- Obtain written certification from each prospective new merchant customer stating the nature of business engaged in by the merchant, form of business organization, how long the merchant (and its principals) have been in business, and how revenue is generated.

- Obtain materials to support the merchant's certification regarding the nature of its business, including, but not limited to, product samples, marketing and advertising materials, copies of the merchant's website, and telemarketing or other sales scripts.
- Obtain materials to support the merchant's certification regarding the form of business organization and longevity, including, corporate formation documents and certificates of good standing from the merchant's state of incorporation.
- Obtain materials to support the merchant's certification regarding sales and revenue information and how revenue is generated.
- Obtain information regarding all current and prior names of the company or its affiliates, including d/b/a/ names. Frequent changes in the merchant's name may indicate involvement in an Internet gambling business.
- Obtain background information regarding all of the company's principals and their involvement in other businesses for at least the previous 2-3 years.
- Determine the physical mailing address of the prospective new merchant customer and whether a significant aspect of the merchant's operations are outside the United States. P.O. Boxes and international mailing addresses or operations may evidence involvement in an Internet gambling business.
- Obtain information regarding the merchant's listings in any business reference sources or publicly available directories.
- Obtain a credit report and/or Dunn & Bradstreet Report on the prospective new merchant customer and its principals.
- Obtain information about the merchant's previous financial institution or payment processing relationships for at least the past two to three years. Then, contact these institutions to determine if the merchant or its principals have ever been terminated, received a high volume of customer complaints, or were involved in wrongful conduct.
- Analyze the prospective new merchant customer's return rates, if applicable, for at least the preceding two to three years. Unreasonably high total return rates or excessive unauthorized return rates may evidence

involvement in an Internet gambling or other unlawful business.[42]

- Determine if the prospective new merchant customer, or any of its principals, has ever been the subject of litigation or government investigation.
- Research consumer protection websites, such as the Federal Trade Commission, Better Business Bureau, or Rip-Off Report websites to determine whether complaints have been lodged against the prospective new merchant customer or its principals.
- Obtain written certification from the merchant that its policies, procedures and actual practices are in compliance with all applicable laws, rules and regulations, including, but not limited to, the UIGEA.

If, after completing its due diligence inquiry, the non-exempt participant makes a determination that the new merchant customer only presents a minimal risk of engaging in an Internet gambling business, pursuant to the Final Rules, the non-exempt participant can open the account without further action.[43] If, however, the non-exempt participant is unable to conclude that the new merchant customer only presents a minimal risk of engaging in an Internet gambling business, the non-exempt participant must obtain certain documentation from the new merchant customer.[44]

The documentation required depends on whether the new merchant customer engages in an Internet gambling business. If the new merchant customer does not engage in an Internet gambling business, it must provide a certification of such fact to the non-exempt participant.[45] If, however, the new merchant customer does engage in an Internet gambling business, the non-exempt participant must obtain both: (1) evidence of the new merchant customer's legal authority to engage in an Internet gambling business, such as a copy of the new merchant customer's license to engage in an Internet gambling business issued by the proper authority, or a reasoned legal opinion that the customer's Internet gambling business does not involve Restricted Transactions, and a written commitment by the merchant to notify the participant of any changes in its legal authority to engage in its Internet gambling business; and (2) a third-party certification that the new merchant customer's systems for engaging in its Internet gambling business are reasonably designed to ensure the Internet gambling business will "remain within the licensed or

otherwise lawful limits, including with respect to age and location verification."[46]

Moreover, pursuant to the Final Rules, a non-exempt participant must notify all of its merchant customers through contract addendums or otherwise that Restricted Transactions are prohibited from being processed by the non-exempt participant.[47]

In addition to the general non-exclusive examples of policies and procedures designed to identify and block Restricted Transactions detailed above, the Final Rules include additional specific examples of procedures to be employed by non-exempt participants in each of the five designated payment systems.[48]

### *The ACH Network*

With respect to the ACH Network, in addition to the due diligence measures discussed above (which apply to new merchant customers and existing customers who the participant has actual knowledge engage in an Internet gambling business), non-exempt participants are required to establish specific procedures to be followed when a participant obtains actual knowledge that its merchant customer has initiated Restricted Transactions.[49] These procedures should address the circumstances under which the merchant customer should be precluded from originating ACH debit transactions or receiving ACH credit transactions, as well as procedures to address the circumstances under which the account should be closed.[50]

As an initial matter, if a non-exempt participant determines that a Restricted Transaction has been initiated prior to the completion of the transaction, the non-exempt participant should halt the transaction and return the funds to the original account. If, however, the non-exempt participant does not determine that a Restricted Transaction has been initiated until after the transaction is complete, the non-exempt participant may want to consider using the funds contained in the merchant customer's reserve account to credit the original accountholder, if known, the amount of the Restricted Transaction. As discussed above, however, it is unclear whether or not the Final Rules require a participant to debit such funds from the merchant and return them to the original accountholder under these circumstances. In any event,

it would be prudent for the non-exempt participant to: (1) provide the merchant customer with written notice that it initiated a Restricted Transaction; (2) warn the merchant customer that its account is subject to termination if it initiates further Restricted Transactions; (3) request written assurance from the merchant that it will not initiate any more Restricted Transactions and is not involved in unlawful Internet gambling; and possibly (4) increase the reserve fund percentage required to be maintained by the offending merchant customer. In order to protect itself from suits by its merchant customers, a participant should incorporate the procedures it establishes regarding the consequences of a merchant initiating Restricted Transactions into a signed agreement with the merchant, whether into the primary agreement or a contract addendum.

Circumstances under which a non-exempt participant should close a merchant customer's account undoubtedly vary depending on the participant and merchant. All non-exempt participants, however, should establish, at a minimum, certain thresholds which when met, require merchant account termination.[51] These thresholds may, among other things, be based on the percentage of total transactions deemed restricted or the number of Restricted Transactions initiated during an established time frame. Such thresholds and the consequences for exceeding them should also be memorialized in a written agreement with the merchant customer, whether in the primary agreement or a contract addendum. Further, if the participant obtains knowledge that the merchant is involved in unlawful Internet gambling or has breached any written assurances made above, the participant should terminate the merchant and consider refraining from paying the merchant amounts that the participant has knowledge are the result of Restricted Transactions. These consequences should likewise be part of a written agreement with the merchant customer.

In addition, although the Final Rules appear to only apply to participants who have a direct relationship with the merchant customer (such as in a traditional third-party processor/merchant relationship), ACH Network participants should also strongly consider applying, as applicable, the above-referenced due diligence and termination policies and procedures to accounts where the processor has an indirect relationship with the merchant, such as with electronic wallets ("e-wallets"),[52] resellers, or independent sales organi-

zations ("ISOs"). Although with these types of relationships the processor typically does not have a direct contractual relationship with the merchant, an ACH Network participant would be prudent to monitor these relationships and the e-wallet, reseller or ISO's conduct so as to not be duped into unwittingly processing Restricted Transactions. At a minimum, an ACH Network participant should require e-wallets, resellers, ISOs and other similar clients to provide written assurance that they are not initiating any Restricted Transactions and are not involved with any merchants who initiate Restricted Transactions or are involved in unlawful Internet gambling. The ACH Network participant should also obtain information regarding the client's policies and procedures it has implemented for complying with the Final Rules (since it is that entity which has the direct relationship with a merchant and is thus required to comply with the Final Rules).

### *The Card System*

Under the Final Rules, a participant in the Card System is deemed to have established policies reasonably designed to identify and block Restricted Transactions if it either: (1) implements the general non-exclusive examples of due diligence procedures referenced above with respect to new customers and customers who the participant has actual knowledge engage in an Internet gambling business; or (2) implements a coding system whereby the transaction code or merchant category code (MCC) accompanying the authorization request for a given transaction can identify and block Restricted Transactions.[53]

Though most Card System participants currently utilize MCCs to identify transactions, and though there exists an MCC for gambling transactions (MCC 7995), two significant hurdles stand in the way of implementing a coding system that does not result in the overblocking of lawful transactions. First, there is no distinct MCC that distinguishes between lawful gambling transactions and Restricted Transactions.[54] Thus, a Card System participant that simply blocks all transactions bearing MCC 7995 runs the risk of blocking legal gambling transactions. Second, the Card System currently has no capability to determine with certainty where a cardholder is located at the time the transaction is made.[55] This inability precludes a participant from selectively permitting specific gambling transactions that may be legal in one

locality and illegal in another.[56]

These challenges to implementing a coding system that does not result in overblocking, however, likely raise a moot point as most Internet gambling businesses that utilize the Card System for funding do so through non-U.S. merchant acquirers that are not subject to the Act or the Final Rules.[57] Moreover, the potential revenue lost to Card System participants as a result of potential overblocking is likely outweighed by the costs such participants would have to incur to comply with requisite due diligence procedures with respect to each of their new or existing merchant customer accounts.

Regardless, however, of whether a participant in the Card System chooses to utilize the coding system, or to design and implement the due diligence procedures contained in the Final Rules, the participant must also establish procedures to be followed when it obtains actual knowledge that a Restricted Transaction has been initiated.[58] Similar to the ACH Network procedures, such Card System procedures should establish the circumstances under which access to the Card System should be denied, and circumstances under which the merchant customer's account should be terminated.[59] These policies and procedures should also be the subject of a written agreement between the participant and its merchant customer, whether in the primary agreement or a contract addendum.

### *The Check Collection System and Wire Transfer System*

Non-exempt participants in the Check Collection and Wire Transfer Systems must also comply with the general due diligence procedures established by the Final Rules for new merchant customers as well as when the participant has actual knowledge that an existing customer engages in an Internet gambling business.[60] Moreover, just as non-exempt participants in the other designated payment systems described above, non-exempt participants in the Check Collection and Wire Transfer Systems must also establish procedures to be followed when they obtain actual knowledge that their merchant customers have initiated Restricted Transactions.[61] These procedures should address the circumstances under which access to the designated payment system should be denied, as well as the circumstances under which a merchant account should be closed, [62] and should be the subject of a written agreement

with the merchant customer.

As noted above, the circumstances under which denial of access to the designated payment system or termination of the merchant account is appropriate is a matter of business judgment and is highly dependent on the existing factual circumstances. Non-exempt participants in the Check Collection and Wire Transfer Systems, however, should at a minimum designate a threshold percentage of allowable Restricted Transactions, that when met, require suspension or termination of the merchant account. These thresholds and the consequences for exceeding them should also be contained in a written agreement with the merchant customer. Moreover, the non-exempt participant should require any merchant customer discovered initiating Restricted Transactions to certify in writing that it acknowledges initiating Restricted Transactions is a violation of its agreement with the non-exempt participant, may subject its account to termination, that the merchant customer will not initiate any more Restricted Transactions, and that the merchant customer is not involved in unlawful Internet gambling.

### *The Money Transmitting System*

Similar to participants in the other designated payments systems, a non-exempt participant in the Money Transmitting System must establish due diligence procedures with respect to account creation and maintenance and must establish procedures addressing the circumstances under which money transmitting services should be denied, or a merchant account should be terminated.[63] As discussed above, the participant's account suspension and termination procedures should be set forth in a written agreement between the participant and its merchant customer, whether in the primary agreement or a contract addendum.

In addition, a non-exempt participant in the Money Transmitting System must also implement procedures regarding ongoing monitoring to detect potential Restricted Transactions, "such as analyzing payments patterns to detect suspicious payment volumes to any recipient."[64] For this ongoing monitoring to be effective, non-exempt participants in the Money Transmitting System should require potential merchant customers to identify the size and frequency of their standard transactions prior to account inception so that the participant will have a baseline with which to compare suspicious transactions. Thereafter,

the non-exempt participant should investigate transactions that vary measurably from the merchant customer's standard transactions, and require the merchant customer to certify that the atypical transaction is not, in fact, restricted.

## Existing Merchant Customers

To comply with the Final Rules, non-exempt participants should, in addition to establishing due diligence procedures with respect to new merchant customers, implement policies and procedures designed to identify and block Restricted Transactions initiated by existing merchant customers. Specifically, non-exempt participants should at a minimum require their existing merchant customers to annually certify that they either: (1) do not engage in an Internet gambling business; or (2) have legal authority to engage in an Internet gambling business. Merchant customers, moreover, should be required to immediately notify the non-exempt participant any time their business changes in a way that has the effect of making the merchant customer's prior certification inaccurate.

Non-exempt participants must also prepare an addendum to their account agreements with existing merchant customers stating that Restricted Transactions are prohibited from being processed through the account or relationship.[65] As with new merchants, the agreement or addendum should also provide that knowingly initiating a Restricted Transaction is grounds for account termination and should set forth the participant's policies and procedures regarding account suspension and termination (including Restricted Transaction thresholds and any policies related to debiting the merchant for transactions later identified as restricted). Moreover, non-exempt participants should consider re-evaluating or re-underwriting questionable existing merchant files in light of the criteria discussed above for new merchants. Additionally, non-exempt participants should monitor return rates, payment transactions, and consumer complaints regarding its existing merchant customers for any suspicious activity. Abnormally high return rates or a sudden change in the nature of payment transactions, for example, may be evidence of Restricted Transactions or other wrongful conduct. Ignoring such potential evidence of Restricted Transactions initiated by existing merchant customers could expose a non-exempt participant to liability for failing to

implement procedures reasonably designed to block Restricted Transactions.

## PENALTIES FOR FAILING TO COMPLY WITH THE FINAL RULES

The UIGEA imposes civil and criminal liability upon Internet gambling businesses that violate the terms of the Act–that is, "persons engaged in the business of betting or wagering" who knowingly accept payment or proceeds in connection with the participation of another person in unlawful Internet gambling.[66] Thus, financial transaction providers are generally immune from direct liability under § 5363. Furthermore, § 5365(d) provides that government actions may not be brought against financial transaction providers to prevent or restrict Restricted Transactions (unless the financial entity is subject to § 5367).[67] Financial transaction providers may, however, be found liable pursuant to § 5367 in the same manner as an Internet gambling business, provided the financial transaction provider (or interactive computer or telecommunications service) has actual knowledge and control of bets and wagers, and: (1) operates, manages, supervises or directs an Internet website at which unlawful bets or wagers may be placed, received, made, or offered to be made; or (2) owns or controls, or is owned or controlled by, any person who operates, manages, supervises, or directs an Internet website at which unlawful bets or wagers may be placed, received, made, or offered to be made.[68]

The Final Rules do not contain specific penalties for non-compliance, nor do they establish a uniform approach to enforcement. The Final Rules, rather, maintain that the compliance requirements are subject to the exclusive regulatory enforcement of the federal functional regulators with respect to the designated payments systems that are subject to the jurisdiction of such regulators.[69] Thus, depending on the whether the non-exempt participant is a national bank, member bank of the Federal Reserve System, bank insured by the Federal Deposit Insurance Corporation ("FDIC"), or savings association, jurisdiction may lie with either: (1) the Office of the Comptroller of the Currency; (2) the Board of Governors of the Federal Reserve System; (3) the Board of Directors of the FDIC; or (4) the Director of the Office of Thrift Supervision.[70] All other non-exempt participants are subject to the jurisdic-

tion of the Federal Trade Commission.[71]

These federal agencies charged with enforcement of the Final Rules "have different enforcement authorities and use different regulatory tools for fulfilling their supervisory responsibilities."[72] It is nearly impossible at this time, therefore, to determine the type and extent of penalty a non-exempt participant may face for failing to comply with the Final Rules. Notwithstanding, by virtue of the Final Rules' reference to regulatory enforcement and assignment of enforcement responsibilities to various federal agencies, it is apparent that some form of liability is contemplated.

Moreover, there also remains a question whether or not financial transaction providers could face liability under general federal and/or state principles of aiding and abetting liability (i.e. aiding and abetting violations of § 5363 by unlawful Internet gambling businesses). Under general aiding and abetting principles, it is well-established that conviction for this offense "requires proof the defendant willingly associated himself with the venture and participated therein as something he wished to bring about."[73] Thus, if a non-exempt participant has knowledge of its merchants' unlawful Internet gambling activities and continues to process Restricted Transactions for the merchants and/or transfer restricted funds to the merchants, the financial transaction provider may be viewed as aiding and abetting a violation of the law by the unlawful Internet gambling business.[74] For example, the government may argue that a non-exempt participant's failure to comply with the written procedures it established regarding the suspension and termination of merchant customer accounts suggests that the non-exempt participant knew of, and intended to aid, the merchant customer's violation of § 5363.[75] Under federal law, aiders and abettors are punished as a principal offender.[76] Accordingly, if a financial entity is found liable as an aider and abettor, it may be subject to the same penalty as the principal Internet gambling business violator of the UIGEA. Whether the government will (or can)[77] seek aiding and abetting liability against financial transaction providers is presently unknown, but this could provide a hook for the government to pursue actions against financial entities, particularly those who continuously process transactions for merchants with knowledge of the merchants' unlawful Internet gambling activities.

## CONCLUSION

The UIGEA and Final Rules represent a frontal assault by the federal government on the growing Internet gambling industry hitting Internet gambling businesses where it hurts most — the wallet. Yet, the costs of implementing the Final Rules are placed squarely on the shoulders of financial transaction providers who are not directly involved in unlawful Internet gambling.

The Final Rules require all non-exempt participants in designated payment systems to implement and comply with extensive due diligence procedures to identify and block Restricted Transactions. Though the Final Rules include non-exclusive examples of procedures financial transaction providers can utilize to comply with their due diligence requirements, the Final Rules for the most part, remain incredibly vague, and give federal regulators great discretion to target and penalize a wide range of financial transaction providers. With the December 1, 2009 deadline for compliance looming, and the penalties for non-compliance with the Final Rules yet unknown, non-exempt financial transaction providers should seek legal advice and closely evaluate their new and existing merchant due diligence and monitoring procedures.

## NOTES

[1] Frank Vandall, *Why We Are Outraged: An Economic Analysis of Internet Gambling*, 7 RICH J. GLOBAL L. & BUS. 291, 291 (2008).

[2] *Compare* Vandall, *supra* note 1, at 291, with Maria Starr, *Internet Gambling Revenues Up 28 Percent,* BODOG BEAT, Mar. 1, 2006, *at* http://www.bodogbeat.com/archives/2006/03/internet_gambling.html.

[3] *Id.*

[4] *Id.*

[5] Unlawful Internet Gambling Enforcement Act of 2006, Pub. L. No. 109-347, Title VIII, § 802, 120 Stat. 1952, (2006) (codified at 31 U.S.C. §§ 5361–67) [hereinafter "UIGEA"].

[6] *Id.* at § 5363.

[7] *But see* UIGEA at § 5367. As discussed in detail below, under § 5367 of the Act, a financial transaction provider may be liable in the same manner as an Internet gambling business if the financial transaction provider has actual knowledge and control of bets and wagers, and: (1) operates, manages, supervises or directs an Internet website at which unlawful bets or wagers may be placed, received, made, or

offered to be made; or (2) owns or controls, or is owned or controlled by, any person who operates, manages, supervises, or directs an Internet website at which unlawful bets or wagers may be placed, received, made, or offered to be made.

[8] *Id*. at § 5364.

[9] *Id.* at § 5363.

[10] 18 U.S.C. § 1804.

[11] 18 U.S.C. § 1952.

[12] 18 U.S.C. § 1955.

[13] 18 U.S.C. §1961. *See also* Andrea L. Marconi and Brian M. McQuaid, *Betting and Buying: The Legality of Facilitating Financial Payments for Internet Gambling*, 124 THE BANKING LAW JOURNAL 486-93 (June 2007), for a detailed discussion of the applicable federal laws and selected state laws regulating Internet gambling.

[14] UIGEA at §§ 5361(b); 5362(1)(E).

[15] Proposed UIGEA Regulations: Burden Without Benefit?: Hearing Before the H. Subcomm. on Domestic and International Monetary Policy, Trade, and Technology, Committee on Financial Services, 110th Cong., 9 (2008) (statement of Louise L. Roseman, Director of the Division of Reserve Bank Operations for the Board of Governors of the Federal Reserve System).

[16] *See* UIGEA at § 5364; *see also generally* 12 CFR § 233 (Treasury Regulations) and 31 CFR § 132 (Federal Reserve Regulations).

[17] *See* Supplementary information issued by the Board of Governors of the Federal Reserve System and the Secretary of the Treasury in conjunction with the Final Rules ("Supplementary Information") at 8.

[18] *See* 12 CFR § 233.3; 31 CFR § 132.3. The Final Rules apply to the Money Transmitting System only to the extent that money transmitting businesses permit customers to initiate a transmission of funds remotely from a location other than the money transmitting business' physical office. Importantly, this definition of the Money Transmitting System precludes check cashing, currency exchange, or the issuance or redemption of money orders, travelers' checks, and other similar instruments. *See* 12 CFR § 233.4(c); 31 CFR § 132.4(c); *see also* Supplementary Information at 13-14.

[19] 12 CFR § 233.3; 31 CFR § 132.3.

[20] 12 CFR § 233.4; 31 CFR § 132.4.

[21] *Id; see also* Supplementary Information at 15. Notwithstanding, a financial transaction provider would be prudent to also monitor its relationships with clients who themselves have the direct merchant customer relationships (such as with electronic wallets and resellers). *See infra* pp. 613-614.

[22] 12 CFR § 233.4(a); 31 CFR § 132.4(a).

[23] 12 CFR § 233.4(b); 31 CFR § 132.4(b).

[24] 12 CFR § 233.4(d); 31 CFR § 132.4(d).
[25] 12 CFR § 233.4(c); 31 CFR § 132.4(c).
[26] *See* Supporting Statement for the Recordkeeping Requirements Associated with Regulation GG (FR 4026; OMB No. 7100-NEW) at 1.
[27] *See* Supplementary Information at 8.
[28] 12 CFR § 233.5; 31 CFR § 132.5; *see also* 12 CFR § 233.2(y); 31 CFR § 132.2(y) (definition of Restricted Transaction).
[29] 12 CFR § 233.2(d); 31 CFR § 132.2(d).
[30] *See* 12 CFR §§ 233.6(c)(iii), (d)(2), (e)(1)(iii), (f)(4), (g)(3); 31 CFR §§ 132.6(c)(iii), (d)(2), (e)(1)(iii), (f)(4), (g)(3).
[31] *See, e.g.,* Letter from Joseph S. Blount of Branch Banking and Trust Company to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System (Dec. 12, 2007), *available at* http://www.federalreserve.gov/SECRS/2007/December/20071213/R-1298/R-1298_118_1.pdf.
[32] 12 CFR § 233.5(c); 31 CFR § 132.5(c).
[33] 12 CFR § 233.5(d); 31 CFR § 132.5(d).
[34] *Id*.
[35] *See* Supplementary Information at 11.
[36] 12 CFR § 233.2(d); 31 CFR § 132.2(d).
[37] 12 CFR § 233.6; 31 CFR § 132.6.
[38] 12 CFR § 233.6(b); 31 CFR § 132.6(b).
[39] 12 CFR §§ 233.6(b)(1), (2)(i); 31 CFR §§ 132.6(b)(1), (2)(i).
[40] 12 CFR § 233.6(b)(4); 31 CFR § 132.6(b)(4).
[41] 12 CFR § 233.6(b)(1); 31 CFR § 132.6(b)(1).
[42] For example, in the ACH Network, pursuant to the NACHA Rules, if a merchant's unauthorized return rate exceeds one percent an investigation is triggered that may result in substantial fines, or forced termination of the merchant. *See* NACHA Rules § 2.18, Appendix 11, § 11.2.1.
[43] 12 CFR § 233.6(b)(2)(i); 31 CFR § 132.6(b)(2)(i).
[44] 12 CFR § 233.6(b)(2)(ii); 31 CFR § 132.6(b)(2)(ii).
[45] 12 CFR § 233.6(b)(2)(ii)(A); 31 CFR § 132.6(b)(2)(ii)(A).
[46] 12 CFR § 233.6(b)(2)(ii)(B); 31 CFR § 132.6(b)(2)(ii)(B).
[47] 12 CFR § 233.6(b)(3); 31 CFR § 132.6(b)(3).
[48] 12 CFR §§ 233.6(c)-233.6(g); 31 CFR §§ 132.6(c)-132.6(g).
[49] 12 CFR § 233.6(c)(1)(iii); 31 CFR § 132.6(c)(1)(iii). *See also* 12 CFR § 233.6(c)(2); 31 CFR § 132.6(c)(2) regarding procedures to follow when a receiving gateway operator or third-party processor has actual knowledge that instructions received from a foreign sender to originate an ACH debit transaction include instructions for Restricted Transactions.

[50] 12 CFR § 233.6(c)(1)(iii); 31 CFR § 132.6(c)(1)(iii).
[51] 12 CFR § 233.6(c)(1)(iii)(B); 31 CFR § 132.6(c)(1)(iii)(B).
[52] *See* Marconi and McQuaid, *supra* note 13, at 496-98 for a detailed discussion of the rise of e-wallets and similar new forms of payment technologies.
[53] 12 CFR § 233.6(d)(1); 31 CFR § 132.6(d)(1).
[54] *See* Letter from Jodi Golinsky of MasterCard Worldwide to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System (Dec. 12, 2007), *available at* http://www.federalreserve.gov/SECRS/2007/December/20071217/R-1298/R-1298_143_1.pdf.
[55] *Id*.
[56] *See* 12 CFR § 233.2(bb); 31 CFR § 132.2(bb).
[57] *See* Supplementary Information at 26.
[58] 12 CFR § 233.6(d)(2); 31 CFR § 132.6(d)(2).
[59] *Id*.
[60] 12 CFR §§ 233.3(e)(1)(i-ii), (g)(1-2); 31 CFR §§ 132.2(e)(1)(i-ii), (g)(1-2).
[61] 12 CFR §§ 233.6(e)(1)(iii), (g)(3); 31 CFR §§ 132.6(e)(1)(iii), (g)(3).
[62] *Id*.
[63] 12 CFR § 233.6(f); 31 CFR § 132.6(f).
[64] 12 CFR § 233.6(f)(3); 31 CFR § 132.6(f)(3).
[65] 12 CFR § 233.6(b)(3); 31 CFR § 132.6(b)(3).
[66] UIGEA at §§ 5363, 5365 (civil remedies), 5366 (criminal remedies).
[67] *Id*. at § 5365(d). This provision, however, is silent regarding after-the-fact claims against financial transaction providers who process Restricted Transactions.
[68] *Id*. at § 5367.
[69] 12 CFR § 233.7(a); 31 CFR § 132.7(a).
[70] *See* 15 U.S.C. 6805(a).
[71] 12 CFR § 233.7(b); 31 CFR § 132.7(b).
[72] *See* Supplementary Information at 28.
[73] *United States v. Zemek*, 634 F.2d 1159, 1174 (9th Cir. 1980); *see also United States v. Groomer*, 596 F.2d 356 (9th Cir. 1979); Marconi and McQuaid, *supra* note 13, at 498-99.
[74] *See Aetna Cas. and Sur. Co. v. Leahey Const. Co., Inc.*, 219 F.3d 519, 536 (6th Cir. 2000) ("[t]he knowledge requirement" can be met, "even though the [defendant] may not have known of all the details of the primary fraud, the misrepresentations, omissions, and other fraudulent practices."); *FDIC v. First Interstate Bank of Des Moines, N.A.*, 885 F.2d 423 (8th Cir. 1989) (bank can be held liable for aiding and abetting a customer who defrauded another bank if bank has a "general awareness" of the customer's fraudulent scheme, notwithstanding the fact that the bank may not have had actual knowledge of the scheme or an intent to participate in the fraud;

general awareness of the fraudulent scheme can be established through circumstantial evidence); *Wells Fargo Bank v. Ariz. Laborers, Teamsters & Cement Masons Local No. 395 Pension Trust Fund*, 201 Ariz. 474, 485 (2002) (because aiding and abetting is a theory of secondary liability, the party charged with the tort must have knowledge of the primary violation, and such knowledge may be inferred from the circumstances); *see also* Marconi and McQuaid, *supra* note 13, at 499.

[75] *Id*.

[76] *See* 18 U.S.C. § 2 ("Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.")

[77] A counterargument exists that a claim of aiding and abetting liability cannot overcome the express exemption in the UIGEA for liability against financial entities. *See* UIGEA at §§ 5363, 5365(d). If such a claim were allowed in the face of existing statutory exemptions then the claim would obviate the need for any exemption–an illogical conclusion. *See* Marconi and McQuaid, *supra* note 13, at 499.