Unlawful Internet Gambling Enforcement Act of 2006
Overview

This document provides an overview of the Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA or Act), 31 USC 5361-5366, and sets forth procedures for reviewing compliance by financial institutions with the joint rule promulgated pursuant to the Act by the Department of the Treasury (Treasury) and the Board of Governors of the Federal Reserve System (Federal Reserve Board). An identical joint rule is published in two parts of the Code of Federal Regulations (12 CFR Part 233 (Federal Reserve Board) and 31 CFR Part 132 (Treasury)). This supervisory guidance is issued by the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency and Office of Thrift Supervision.

Summary

The Act prohibits gambling businesses from knowingly accepting payments in connection with the participation of another person in a bet or wager that involves the use of the Internet and that is unlawful under any federal or state law (termed "restricted transactions" in the Act). The Act also requires Treasury and the Federal Reserve Board (in consultation with the U.S. Attorney General) to promulgate regulations requiring certain participants in payment systems that could be used for unlawful Internet gambling to have policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit the processing of restricted transactions. These regulations are independent of any other regulatory framework, such as the Bank Secrecy Act or consumer protection regulations.

A joint rule has been issued by Treasury and the Federal Reserve Board that designates five payment systems as covered by the Act. The designated payment systems are (i) automated clearing house (ACH) systems, (ii) card systems, (iii) check collection systems, (iv) money transmitting businesses, and (v) wire transfer systems.

The rule requires certain participants in the designated payment systems to establish policies and procedures that are reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions. A "participant" is defined as "an operator of a designated payment system, a financial transaction provider that is a member of or, has contracted for financial transaction services with, or is otherwise participating in, a designated payment system, or a third-party processor." The term "participant" does not include a participant's customer unless the customer is also a financial transaction provider participating on its own behalf in the designated payment system.

The rule exempts certain participants from the requirement to have policies and procedures, but exempt participants are not specifically identified. Rather, all participants in designated payment systems are exempt from the requirements unless they are specifically enumerated in the rule as "non-exempt" (see chart at Attachment B). In general, non-exempt participants are those that establish or maintain accounts for commercial customers and are in a position to conduct due diligence on the customer. There are, however, no exemptions for card system participants

because card systems usually have a transaction coding system that would permit potential restricted transactions to be segregated by participants during the authorization process.

Finally, the rule provides non-exclusive examples of acceptable policies and procedures. The examples are not the only means of complying with the rule, but they provide a safe harbor for non-exempt participants in the designated payment systems. Because variations among federal and state laws and interpretations preclude a uniform definition of "unlawful Internet gambling," the rule does not contemplate that participants in designated payment systems (other than card systems) would be able to monitor transactions and identify restricted transactions. Rather, the rule focuses on due diligence to be conducted by financial institutions and third-party processors in establishing and maintaining commercial customer accounts. Card systems are the only designated payment systems that commonly use a merchant and transaction coding framework that may permit participants to identify and block, during processing, transactions with indicia of being restricted transactions. Accordingly, card systems are the only payment systems for which the joint rule suggests that transactions could be blocked during processing.

The following sections provide additional information about the systems, participants, and policies and procedures described in the rule. More detailed explanation can be found in the final rule published in the Federal Register (73 FR 69382, November 18, 2008). A summary chart of the obligations of non-exempt participants is found at Attachment B. Examination procedures are found at Attachment C.

1. Designated Payment Systems and Non-Exempt Participants

The rule designates five payment systems that may be used for restricted transactions: card systems, ACH systems, wire transfer systems, check collection systems, and money transmitting businesses. Participants in each system are exempt unless specifically listed in the rule as non-exempt; however, no card system participants are exempt. In general, participants in a designated payment system are exempt unless they have direct relationships with commercial customers. In addition, the rule covers only U.S. offices of payment system participants.[1]

Card Systems. The rule covers all card systems, including credit, debit, and stored value. Various participants in a card system transaction have responsibilities under the non-exclusive examples provided in the joint rule for card systems.

ACH, Check Collection, Wire Transfer, and Money Transmitting Businesses Systems. For ACH, wire transfer, check collection, and money transmitting businesses systems, the rule focuses only on due diligence on accounts that are held directly for commercial customers. Participants in these payment systems that have direct relationships with a commercial customer can assess the risk, if any, that the customer is engaged in unlawful Internet gambling. Such participants and third-party processors are non-exempt and should have reasonably designed policies and procedures to prevent or prohibit restricted transactions.

[1] References in this document to banks and depository institutions should be understood to include all financial institutions supervised by the issuing agencies, including banks, thrifts, credit unions and non-bank subsidiaries.

The payment system participants responsible for establishing policies and procedures reasonably designed to prevent or prohibit restricted transactions are as follows:

- ACH systems –
    - In domestic ACH transactions, the depository financial institution and any third-party processor receiving the credit or initiating the debit on behalf of the commercial customer.
    - In cross-border ACH debit transactions, the receiving gateway operator and any third-party processor that receives instructions directly from a foreign sender.
- Card systems – the card system operator, merchant acquirers, third-party processors, and card issuers.
- Check collection systems – the depositary bank.
- Money transmitting businesses – the operator.
- Wire transfer systems – the beneficiary's bank.

Third-party processors. The rule provides that third-party processors may be participants in designated payment systems, and that any non-exempt third-party processor must establish policies and procedures as required by the rule. Thus, for purposes of UIGEA, third party processors have their own compliance obligations independent of the obligations of financial institutions. Under the rule, a third-party processor is a service provider that:

(1) In the case of a debit transaction payment, such as an ACH debit entry or card system transaction, has a direct relationship with the commercial customer that initiates the debit transfer transaction and acts as an intermediary between the commercial customer and the first depository institution to handle the transaction;
(2) In the case of a credit transaction payment, such as an ACH credit entry, has a direct relationship with the commercial customer that is to receive the proceeds of the credit transfer and acts as an intermediary between the commercial customer and the last depository institution to handle the transaction; or
(3) In the case of a cross-border ACH debit or check collection transaction, is the first service provider located within the U.S. to receive the ACH debit instruction or check for collection.

A service provider simply providing back-office support to a financial institution is not a "third party processor" under the rule, but the financial institution should ensure that the service provider complies with the institution's policies.

Correspondent relationships. The rule generally covers payments flowing through foreign correspondent relationships. For example, a correspondent bank that participates in wire transfer transactions is non-exempt when it is acting as the beneficiary's bank. If a U.S. depository institution establishes a correspondent account for a foreign financial institution that will involve designated payment system(s) for which the U.S. bank will be a non-exempt participant, the U.S. bank must have policies and procedures in place as required by the rule.

2. Policies and Procedures

The rule requires all non-exempt participants in designated payment systems to establish and implement policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions. Neither the Act nor the rule imposes a strict liability standard with respect to the processing of restricted transactions. Participants are permitted to design and implement policies and procedures tailored to their operations and may use different policies and procedures with respect to different business lines. The rule provides examples of reasonably designed policies and procedures that would meet the requirements of the rule for each designated payment system. While these policies and procedures are not the exclusive means of compliance, they will be treated as a safe harbor for purposes of regulatory compliance.

System policies and procedures. For operator-driven systems, such as card systems, the operator may have policies and procedures in place to comply with the rule. For purposes of regulatory compliance, the Act and the rule permit a participant in such a system to either establish its own policies and procedures or to rely on and comply with conforming policies and procedures of the system operator. In this regard, a non-exempt participant may rely on a written statement or notice from the operator that the system operator's policies and procedures are designed to comply with the rule, unless and until the participant is notified by its regulator that the operator's policies are not compliant and should not be relied upon. If a non-exempt participant relies on such a statement from the operator and is in compliance with the system operator's policies and procedures, the participant would not be expected to design its own policies and procedures for transactions through that system.

Notice to commercial accountholders. Within its due diligence examples, the rule contemplates that non-exempt participants in designated payment systems would provide to all commercial accountholders (both for new accounts and for existing accounts) notice that restricted transactions are prohibited from being processed through the account or relationship. The rule provides various examples of methods for providing notice, such as through provisions in the account or relationship agreement, a separate notice, including information on the participant's website, or otherwise.

General due diligence approach. The rule provides a safe harbor that focuses on a due diligence process in establishing a commercial customer relationship as the core policy and procedure for reducing the risk that restricted transactions will be introduced into the payment system. The rule's non-exclusive examples of reasonably designed policies and procedures contemplate a risk-based approach to due diligence for commercial accountholders. Under the rule, adequate due diligence on a commercial account could include the following:

1. At the establishment of the customer relationship, the institution should conduct due diligence on the customer and determine whether the customer poses a minimal risk of engaging in an Internet gambling business. (For example, if a company does not engage in any Internet business, no further inquiry would be necessary.) Certain entities are defined in the rule as posing minimal risk, such as agencies, departments or divisions of federal or state government and entities directly supervised by a Federal functional regulator (*e.g.*, banks, savings associations, credit unions, broker-dealers, etc.). If the

institution's normal account-opening due diligence indicates that the customer poses a minimal risk of engaging in an Internet gambling business, no further due diligence need be done.

2. If the institution cannot determine whether the commercial accountholder poses a minimal risk of engaging in an Internet gambling business, then the institution should obtain the following documentation from the customer:

    a. A certification from the customer that it does not engage in an Internet gambling business; or
    b. If the customer does engage in an Internet gambling business:
        i. Either a copy of the commercial license from a State or tribal authority authorizing the customer to engage in the business or a reasoned legal opinion (as defined in the rule) that demonstrates that the business does not involve restricted transactions; and
        ii. A written commitment by the customer to advise the participant of any changes in its legal authority to engage in the Internet gambling business; and
        iii. A third-party certification that the customer's systems for engaging in the Internet gambling business are reasonably designed to ensure that the business will remain within legal limits.

Actual knowledge of Internet gambling business. Under the rule's safe harbor for use whenever a participant has actual knowledge that an existing commercial customer is engaging in an Internet gambling business, the participant should have procedures to obtain from the accountholder the documentation appropriate for commercial customers that present more than a minimal risk of engaging in Internet gambling and who cannot certify that they are not engaging in an Internet gambling business.

Actual knowledge of restricted transactions. Under the rule's safe harbor for use whenever a participant has actual knowledge that a commercial customer has engaged in restricted transactions, the participant should have procedures to be followed relating to continued transaction processing, account review, suspicious activity filing, and account closure. The rule does not specify when transactions must be limited or accounts closed, only that the institution should have procedures in place. The appropriate Federal financial institution regulator has discretion to impose requirements in the course of supervision or within the context of an enforcement action.

In determining whether a financial institution or third-party processor has "actual knowledge," the rule contemplates that it would receive reliable information about both the transactions and their illegality from a source such as a government agency. Financial institutions are not required by UIGEA to proactively collect information independently to develop actual knowledge of restricted transactions.

In general, a U.S. participant that is the first U.S. entity in the chain to process an inbound cross-border debit transaction[2], such as an ACH debit or check, should have procedures in place for when it obtains actual knowledge that a foreign sender has sent instructions for restricted transactions. For example, it may send notification to the foreign sender (the rule includes sample notice language).

Relationship to Bank Secrecy Act/Anti-Money Laundering Compliance. The preamble to the rule notes that participants may implement due diligence procedures by incorporating them into existing account-opening due diligence procedures, for example, under Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance processes. However, regardless of how and where within its compliance function or management structure a financial institution chooses to place responsibility for UIGEA compliance, UIGEA compliance is separate and independent from the legal scope of BSA/AML requirements, the BSA/AML program rule, and examination mandates for BSA/AML compliance programs. Compliance with UIGEA does not fulfill any other compliance requirements, including, for example, requirements to file Suspicious Activity Reports (SARs). If any depository institution suspects that a customer is processing illegal transactions, including restricted transactions, through the depository institution's facilities, the depository institution should file a SAR with the appropriate authorities.

3. Safe Harbors for Designated Payment Systems

The rule gives examples of policies and procedures for each payment system, generally by reference to the overall due diligence approach. These policies and procedures are not the exclusive means of compliance with the rule, but constitute a safe harbor for compliance.

Card systems. Card issuers, system operators, merchant acquirers, and third-party processors are in compliance with the rule if their policies and procedures do the following:

- (1) Apply the due diligence procedures set forth in the rule to accounts or relationships established on or after the rule's compliance date and provide notice to all commercial accountholders of the prohibition on conducting restricted transactions, and
  (2) Apply the due diligence requirements set forth in the rule if the institution has actual knowledge that a commercial customer engages in an Internet gambling business; OR

- Implement a system of codes (such as for transactions and merchant/business categories) in which
  - The system permits the operator or card issuer to identify and deny authorization for payments that may be restricted transactions; and
  - The system operator has procedures to detect potential restricted transactions, test for proper coding, and monitor payment patterns;

For card system operators, merchant acquirers and third-party processors, policies and procedures must address instances in which the institution has actual knowledge that a merchant

[2] The rule exempts institutions processing outbound cross-border ACH credit transactions and wire transfers.

has received restricted transactions through the card system. The procedures should address when system access should be denied and when the merchant account should be closed.

ACH systems. Originating depository financial institutions (ODFIs) and third-party processors are in compliance with the rule if their policies and procedures do the following:

- Apply the due diligence procedures set forth in the rule to commercial accounts or relationships established on or after the rule's compliance date and provide notice to all commercial accountholders of the prohibition on conducting restricted transactions. If the account is a foreign correspondent banking relationship, the due diligence should determine whether the foreign financial institution presents more than a minimal risk of engaging in an Internet gambling business;
- Apply the due diligence requirements set forth in the rule if the institution has actual knowledge that a commercial customer engages in an Internet gambling business; and
- Address instances where the institution has actual knowledge that restricted transactions have been processed through an account.

For cross-border transactions, institutions that receive inbound debits directly from a foreign sender should have policies and procedures for notifying any non-U.S. correspondent institution if the U.S. receiving institution (RDFI) has "actual knowledge" of restricted transactions passing through the correspondent account. For the purposes of UIGEA, depository institutions are not expected to conduct due diligence on a foreign financial institution's commercial customers. However, if a U.S. institution obtained actual knowledge that its foreign correspondent's customer sent restricted transactions through an account at the U.S. institution, the institution would notify its foreign correspondent of the restricted transaction. Such notification should contain enough detail (including identifying intermediaries) to describe the transaction's path to the foreign correspondent counterparty.

Wire transfer systems. Beneficiary's banks are in compliance with the rule if their policies and procedures do the following:

- Apply the due diligence procedures set forth in the rule to commercial accounts or relationships established on or after the rule's compliance date and provide notice to all commercial accountholders of the prohibition on conducting restricted transactions;
- Apply the due diligence requirements set forth in the rule if the institution has actual knowledge that a commercial customer engages in an Internet gambling business; and
- Address instances in which the institution has actual knowledge that restricted transactions have been processed through an account.

Check collection systems. Depositary banks are in compliance with the rule if their policies and procedures do the following:

- Apply the general due diligence procedures set forth in the rule to commercial accounts or relationships established on or after the rule's compliance date and provide notice to all commercial accountholders of the prohibition on conducting restricted transactions;

- Apply the due diligence requirements set forth in the rule if the institution has actual knowledge that a commercial customer engages in an Internet gambling business; and
- Address instances in which the institution has actual knowledge that restricted transactions have been processed through an account.

For cross-border transactions, the first institution to receive a check from a foreign sender should have policies and procedures for notifying the sender if the institution has actual knowledge that the check constituted a restricted transaction. Such notification should contain enough detail (including identifying intermediaries) to describe the transaction's path to the foreign correspondent counterparty.

Money transmitter businesses. Operators of a money transmitting business that permit customers to initiate transmission of funds remotely, such as via the Internet or telephone, are in compliance with the rule if their policies and procedures do the following:

- Apply the general due diligence procedures set forth in the rule to commercial accounts or relationships established on or after the rule's compliance date and provide notice to all commercial accountholders of the prohibition on conducting restricted transactions;
- Apply the due diligence requirements set forth in the rule if the institution has actual knowledge that a commercial customer engages in an Internet gambling business;
- Conduct ongoing monitoring and testing to detect potential restricted transactions; and
- Address instances where the institution has actual knowledge that restricted transactions have been processed through an account.

4. Effective Dates

The rule's effective date of January 19, 2009, refers only to the date of publication in the Code of Federal Regulations. Compliance with the rule is required as of June 1, 2010.

As of June 1, 2010, institutions following the rule's examples of policies and procedures should have provided notice to their commercial accountholders.

As of June 1, 2010, participants relying on system policies and procedures should have obtained a statement from the operator.

For all commercial accounts established on or after June 1, 2010 (including accounts for existing customers), institutions should follow established due diligence policies and procedures. Institutions should also follow due diligence policies and procedures if they have actual knowledge that an existing commercial customer is engaging in an Internet gambling business.

Attachment B

UIGEA: Designated Payment Systems and Requirements of Participants

Payment System	Non-Exempt Participants	Safe Harbor Policies and Procedures: General Requirements
Card Systems (credit, debit, stored value)	1. Card issuers 2. Merchant acquirers 3. Operators 4. Third-party processors	• Due diligence or • Use of codes to identify restricted • transactions and ongoing monitoring for codes; and • Restricted transactions procedures.
Automated Clearing House	1. RDFI, credit transactions 2. ODFI, debit transactions 3. Gateway operator for cross-border debits 4. Third-party processors for any of 1, 2, or 3	• Due diligence; • Restricted transaction procedures; and • For inbound cross-border ACH debit transactions, notice to correspondent bank in case of actual knowledge of restricted transactions.
Wire Transfer	Beneficiary's bank	• Due diligence and • Restricted transactions procedures.
Check Collection	1. Depositary bank 2. First U.S. bank for cross-border check receipts	• Due diligence; • Restricted transactions procedures; and • For cross-border transactions, notice to correspondent bank in case of actual knowledge of restricted transactions.
Money Transmitting Businesses	Operators of money transmitting businesses that permit initiation of funds transmissions remotely, such as via Internet or telephone.	• Due diligence; • Ongoing monitoring by the operator to detect potential restricted transactions; and • Restricted transactions procedures.

"Due diligence" includes the following:

- Written notice to all commercial accountholders that the account must not be used for restricted transactions; and
- Risk assessment for each commercial account opened on or after the rule's compliance date to determine whether the accountholder poses more than a minimal risk of engaging in restricted transactions; and
- Obtaining required documentation if the commercial customer presents more than a minimal risk of engaging in an Internet gambling business and cannot certify that it is not so engaged or if the institution has actual knowledge that a commercial accountholder is engaged in an Internet gambling business.

"Restricted transactions procedures" are to be followed when an institution has actual knowledge that a commercial customer has received funds in a restricted transaction. Procedures should address continued transaction processing, account review, SAR filing, and account closure.

Examination Procedures
Unlawful Internet Gambling Enforcement Act

Examination work to review a supervised institution's compliance with UIGEA may be conducted independently or together with reviews in other operational or compliance areas, *e.g.*, information technology or BSA/AML compliance. Examiners should note, however, that regardless of how the examination work is carried out, the requirements of UIGEA are independent of other regulatory frameworks. For example, even if UIGEA compliance is handled by an institution's BSA compliance area, it is not a BSA program requirement, it is not covered by the mandates of 12 USC 1818(s), and it does not supersede any other compliance requirements.

UIGEA compliance examination should be risk-focused. In tailoring the scope of the examination work, examiners may consider appropriate risk factors, such as the number of commercial accounts the institution maintains for commercial customers engaged in the business of internet gambling. If the institution is not using the safe harbor policies and procedures as set forth in the rule and as assumed in the examination procedures below, examiners must determine whether the institution's policies and procedures are reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions.

1. Determine whether the institution qualifies as a non-exempt participant in a designated payment system as defined by the provisions of the UIGEA (see chart at Attachment B).

2. Obtain and review any risk or other assessments and audit reports that assess the institution's UIGEA compliance.

3. Determine which position in the institution is responsible for UIGEA compliance.

4. Obtain the institution's policies and procedures for UIGEA compliance.

    a. Review the adequacy of the institution's policies and procedures for determining whether a commercial customer presents more than a minimal risk of engaging in an Internet gambling business.

    b. Review the adequacy of the institution's policies and procedures for obtaining documentation from commercial customers who present more than a minimal risk of engaging in an Internet gambling business, or when the institution has actual knowledge that the customer is engaged in such a business. Documentation includes:
        i. A certification from the customer that it does not engage in an Internet gambling business; or
        ii. If the customer does engage in an Internet gambling business:
            1. Either a copy of the commercial license from a State or Tribal authority authorizing the customer to engage in the business or a reasoned legal opinion that demonstrates that the business does not involve restricted transactions; and

2. A written commitment by the customer to advise the participant of any changes in its legal authority to engage in the Internet gambling business; and
3. A third-party certification that the customer's systems for engaging in the Internet gambling business are reasonably designed to ensure that the business will remain within legal limits.

c. If applicable, determine whether the institution appropriately uses a code system for card transactions to detect potential restricted transactions.

d. Determine whether the institution has in place:
    i. An adequate mechanism to receive notice (*e.g.*, from law enforcement or supervisory authorities) that restricted transactions have been sent through an account at the institution, and
    ii. Policies and procedures to be followed when the bank receives such actual knowledge of restricted transactions.

e. Review the adequacy of any procedures or measures established by the institution to determine the circumstances under which the institution should deny service, close an account, report suspicious activity, conduct an account review or continue transaction processing in instances of actual knowledge of restricted transactions.

f. Determine whether the institution has taken appropriate steps to provide written notice (as part of an account agreement, on the institution's website or otherwise) to all commercial accountholders that accounts may not be used for restricted transactions.

g. Determine whether the institution has incorporated UIGEA compliance measures into its processes for managing correspondent account relationships.