RED FLAGS

PROTECTING CUSTOMER ACCOUNTS FROM IDENTITY FRAUD: IS YOUR CASINO COMPLIANT?

BY DAVID D. WADDELL
AND DOUGLAS L. MINKE

The casino industry is unique when it comes to the relationship operators have with their customers. Commercial and Native American casino operations across the United States have invested billions of dollars to establish safe, comfortable and secure environments for their patrons to enjoy a dynamic entertainment experience. In addition to world-class leisure amenities that are offered in the modern casino environment, the core service provided by casinos continues to be a secure and regulated gaming experience.

As a result of the unique nature of the casino environment, numerous laws categorize casinos as financial institutions and require reporting of various financial transactions, to prevent these businesses from being used by unscrupulous people for laundering money, evading taxation or funding criminal activities.

Casinos across the country have developed sound practices to ensure compliance with the anti-money laundering provisions of the Bank Secrecy Act/Title 31 and the Patriot Act. Despite the fact that casino operators have developed systems to ensure a safe experience, new regulations continue to be adopted that, if not complied with, could expose operators to regulatory fines and/or civil/criminal liability.

Starting in 2010, certain casino operators that offer specific types of financial accounts will be required to develop policies and procedures to prevent identity theft. According to a 2010 congressional report, identify theft is the fastest-growing type of fraud in the United States. In 2008, an estimated 9.9 million Americans were victims of identify theft, an increase of 22 percent from 2007. The Federal Trade Commission estimates that identity theft costs consumers approximately $50 billion annually. As a result, the FTC is implementing a new "Red Flags Rule" to seek assistance from businesses to prevent identity theft.

There is a lot of confusion within the gaming industry over these matters. The purpose of this article is to provide some clarity with regard to the changes in federal law, and to provide a general overview of the steps casinos should take to assure ongoing compliance.

Jim Dowling, a former anti-money laundering official with the United States Office of National Drug Control Policy and currently president of Dowling Advisory Group (a company that has extensive experience in auditing and assisting companies in federal compliance matters), states that "identify theft continues to plague many different industries, and is a growing concern with companies that store customer information electronically." Dowling says current cases show where a single breach can result in thousands of individuals' personal information being compromised. Beginning June 1, after four extensions of the enforcement date, the FTC is scheduled to begin enforcing the Red Flags Rule, a set of identity theft prevention regulations issued pursuant to the Fair and Accurate Credit Transactions Act. The Red Flags Rule, which is codified at 16 C.F.R. §681.1, generally requires: **the development and implementation of a written identity theft protection program that is designed to detect, prevent and mitigate identity theft**; and **the periodic performance of a risk assessment to determine whether the business offers or maintains any other accounts for which there is a "reasonably foreseeable risk" to customers or to the business from identity theft.**

IS YOUR CASINO SUBJECT TO THE RED FLAGS RULE?

The Red Flags Rule is applicable to "financial institutions" and/or "creditors" that maintain "covered accounts."

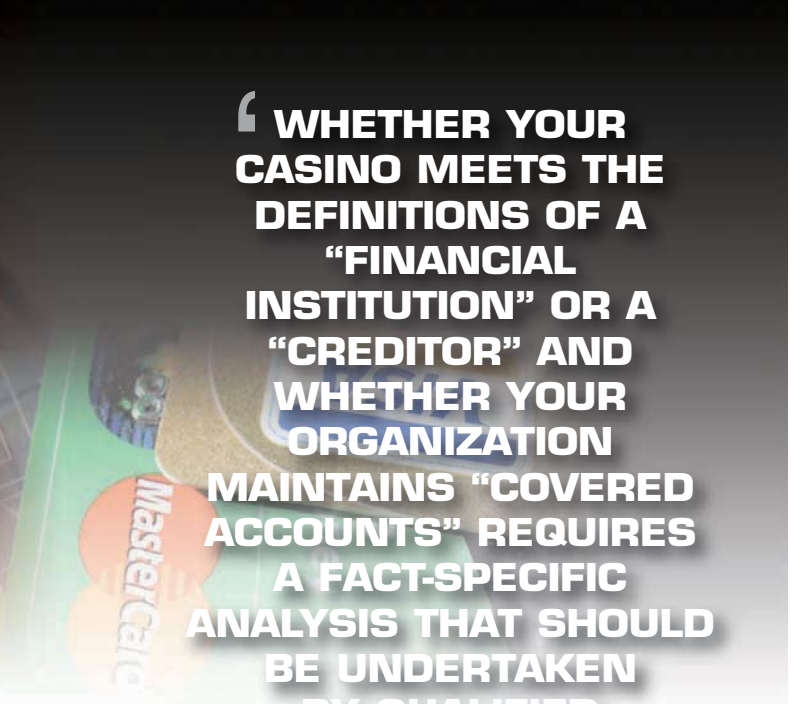
For the purposes of the Red Flags Rule, a "financial institution" is defined as "a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other person that, directly or indirectly, holds a transaction account (as defined in 12 U.S.C. §461(b)) belonging to a consumer."

Many casino operators will not likely meet the definition of a "financial institution" for purposes of the Red Flags Rule. It is important to note that the analysis does not end there, as the identity theft prevention regulations also cover entities that are considered "creditors."

A "creditor" is "any person who regularly extends, renews or continues credit; any person who regularly arranges for the extension, renewal or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew or continue credit."

It is this definition of "creditor" which may bring many casino operators within these regulatory confines.

An organization that qualifies as either a "financial institution" *or* a "creditor" must then analyze its internal operations to determine whether it maintains "covered accounts," which are defined as:



> “WHETHER YOUR CASINO MEETS THE DEFINITIONS OF A “FINANCIAL INSTITUTION” OR A “CREDITOR” AND WHETHER YOUR ORGANIZATION MAINTAINS “COVERED ACCOUNTS” REQUIRES A FACT-SPECIFIC ANALYSIS THAT SHOULD BE UNDERTAKEN BY QUALIFIED LEGAL COUNSEL.”

> **(i)** an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and
>
> **(ii)** any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

The determination of whether your casino meets the definitions of a “financial institution” or a “creditor” and whether your organization maintains “covered accounts” requires a fact-specific analysis that should be undertaken by qualified legal counsel.

Percival Veloro, senior gaming auditor of the Agua Caliente Band of Cahuilla Indians, says the “formal adoption of a Red Flags Rule written program is key to properly protecting the casino and its customers from the risk of identity theft and assuring compliance with federal law.” The Agua Caliente Band recently implemented Red Flags Rule compliance procedures.

Although the implementation of any new federal requirement can sometimes seem daunting, experience in working on such programs reveals that they are not too difficult to develop. Existing casino compliance systems help minimize the risk of identity theft in most casino operations. Proper documentation of the written program is a key first step, and the guidance of legal counsel in this uncharted territory will provide the casino with reassurance that all legally required steps are being taken.

NUTS AND BOLTS OF RED FLAGS RULE COMPLIANCE

The seminal part of Red Flags Rule compliance centers on the development and implementation of a written identity theft prevention program “that is designed

"A CASINO SHOULD DESIGNATE AN APPROPRIATE INDIVIDUAL OR COMMITTEE TO OVERSEE THE RED FLAGS RULE COMPLIANCE PROGRAM."

to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account."

"Establishing a robust Red Flags Rule program can help casinos secure their customers' information," says Dowling, "and mitigate potential federal and state regulatory sanctions, as well as civil liability."

According to the regulations, a program must be appropriate to the size and complexity of the business operation and must include reasonable policies and procedures to:

- identify relevant red flags (pattern, practice or specific activity that indicates the possible existence of identity theft), and incorporate those red flags into the program;
- detect red flags that have been incorporated into the program;
- respond appropriately to any red flags that are detected to prevent and mitigate identify theft; and
- ensure the program is updated periodically to reflect changes in risks to customers.

The categories of identity theft-related "red flags" that a subject business should be cognizant of include, but are not limited to:

- alerts, notifications or other warnings received from consumer reporting agencies (such as a fraud alert, notice of credit freeze or address discrepancy included in a consumer credit report);
- presentation of suspicious documents from a patron (including documents that have been forged or altered, or if the photograph on an identification document is not consistent with the patron's appearance);
- presentation of suspicious identifying information (e.g. suspicious address change, a Social Security number that had not been issued, or is outside the corresponding date-of-birth range, fictitious phone number);
- unusual use of, or suspicious activity related to, a covered account (activity on the account not consistent with past record of use, material increase in available credit line, mail to patron returned "undeliverable" although transactions continue to be conducted from the account); and
- notice from patrons, identity theft victims, law enforcement or other persons regarding possible identity theft.

In addition to the development and implementation of the program, Red Flags Rule compliance also requires the periodic performance of a "risk assessment" to determine whether the business offers or maintains any other accounts for which there are reasonably foreseeable risks to customers or to the business from identity theft.

In conducting this periodic risk assessment, a business must take into account: (i) the methods it provides to open its accounts, (ii) the methods it provides to access its accounts, and (iii) its previous experiences with identity theft.

Veloro also emphasizes that "a written program demonstrates that the casino has given the topic thoughtful analysis, meeting the requirements of federal law."

Dowling notes that "as with all compliance programs, the first step to establishing an effective program is to prepare a risk assessment."

INTEGRATING RED FLAGS RULE COMPLIANCE

A casino which is subject to the Red Flags Rule must craft a compliance program that will comfortably fit within and further complement its overall gaming regulatory compliance procedures. This process will include drafting internal controls, assembling departmental operating procedures and obtaining the necessary gaming regulatory approvals of such changes.

Also, a casino should designate an appropriate individual or committee to oversee the Red Flags Rule compliance program. For purposes of efficiency, and also to draw on existing institutional compliance knowledge, these oversight duties can be delegated to the existing compliance officer. However, a different designated employee, the board of directors, or a committee of the board can also be charged with Red Flags Rule compliance.

Those charged with administering the compliance program should report, at least annually, to the casino's board of directors, a committee of the board or a designated member of senior management on Red Flags Rule compliance.

Current employee training to ensure compliance with Title 31/Bank Secrecy Act provisions, the mandates of the Office of Financial Assets Control and other gaming regulatory requirements should be expanded to include proper implementation, administration and monitoring of the Red Flags Rule compliance program. Current internal and external audits of the compliance programs should also be expanded to include auditing of the identity theft prevention program.

Finally, the Red Flags Rule compliance program should also be periodically reviewed and revised to stay current for developments in the gaming industry, as well as to take into account identity theft instances experienced by the casino.

Notably, Veloro also states, "It is our goal that our Red Flags Rule compliance program will protect the casino against potential liability for penalties or for damages that might result from identity theft."

PENALTIES FOR NON-COMPLIANCE

Red Flags Rule compliance should be an integral part of a casino's overall compliance program. In addition to the gaming-related compliance concerns, the FTC is authorized to seek civil penalties and injunctive relief against subject businesses for regulatory violations. The current maximum civil penalty for non-compliance with the Red Flags Rule is $3,500 per violation. However, a more important reason for compliance is to provide a safe and secure wagering and entertainment environment. A sound identity theft prevention program assures your casino patrons that your property is doing its part to protect their identities.

KEY RESOURCES

For additional information concerning the FTC and its enforcement of the Red Flags Rule, visit www.ftc.gov/redflagsrule. Interested persons can also visit RMC Legal's website (www.rmclegal.com) and download a recent webinar presentation that discussed compliance issues related to the Bank Secrecy Act, the Office of Foreign Assets Control and the Red Flags Rule, as well as to register for a May 5 webinar titled, "You Think Your Casino is Compliant—Will an IRS Auditor Agree?"

David Waddell is an attorney and president of Regulatory Management Counselors, P.C. Waddell's areas of practice include gaming law, Title 31 compliance, business, tax and municipal law. He also sits on the editorial board for the Gaming Law Review *and* Global Gaming Business *and has been listed in* Best Lawyers in America *for gaming. He can be reached at 517-507-3859, or at waddell@rmclegal.com.*

Douglas Minke is an attorney with Regulatory Management Counselors, P.C. Minke's areas of practice include general business law, gaming supplier licensing, commercial litigation and creditors' rights. You can reach Minke at 313-221-9380, or minke@rmclegal.com, or online at www.rmclegal.com.