Getting in the Game: A Guide to Successful Gaming Company Compliance
TABLE OF CONTENTS

Authors Page

Chapter 1  SURVIVAL OF THE FITTEST: GOING BEYOND COMPLIANCE ................................................................. 1

Chapter 2  WINNING PRINCIPLES: ATTRIBUTES OF A SUCCESSFUL COMPLIANCE PLAN .......................... 3

Chapter 3  THE KEY PLAYERS IN THE COMPLIANCE GAME ........... 7

Chapter 4  HOW TO MAKE YOUR PLAN FUNCTION .................... 12

Chapter 5  WHISTLEBLOWER PROCESS AND SARBANES-OXLEY ACT REQUIREMENTS .................. 21

Chapter 6  INTERNAL INVESTIGATIONS: LACK OF A PLAN CAN BE RISKY .......................................................... 29

Chapter 7  RISK APPETITE: DETERMINING YOUR DIET PLAN...... 36

Chapter 8  INTERNAL AUDIT ROLE: A SOLID FOUNDATION FOR SUCCESS ......................................................... 41

Chapter 9  THE REGULATORY COMPLIANCE AUDIT ................. 46

Chapter 10 SECURITIES ISSUES: INSIDER TRADING AND FALSE OR MISLEADING DISCLOSURE .......... 50

Chapter 11 BANK SECRECY ACT AND ANTI-MONEY LAUNDERING ............................................................... 56

Chapter 12 CAMPAIGN CONTRIBUTIONS ........................................ 62

Chapter 13 FOREIGN CORRUPT PRACTICES ACT: KNOW THE RULES OF THE GAME IN EMERGING MARKETS ....... 66

Chapter 14 ANTITRUST ISSUES: HOW TO AVOID THE MONOPOLY GAME ...................................................... 72

Chapter 15 ADVERTISING AND MARKETING: KEEP IT COMPLIANT ................................................................. 79

Chapter 16 CONFLICTS OF INTEREST: THE IMPORTANCE OF MAINTAINING INDEPENDENCE .................. 82

Chapter 17 MONEY LAUNDERING .................................................... 87

Conclusion  THE END OF THE GAME .............................................. 91

Copyright—all rights reserved®

Much of the material in this document originally appeared in Casino Enterprise Management magazine.

This publication should not substitute for the advice of competent legal counsel or your professional services advisor.
AUTHORS

Anthony Cabot, Lewis and Roca LLP, co-author
Anthony Cabot leads Lewis and Roca’s gaming practice. He has played a strategic and integral role in the development of gaming laws and regulations for the past quarter century. In addition to representing several major casino companies and suppliers; he has authored or edited eight books on gaming law. He is a founder and the current president of the International Masters of Gaming Law and an adjunct Professor of Law at the Boyd School of Law at the University of Nevada, Las Vegas. Tony Cabot is listed among The Best Lawyers in America® 2005-2006, by Woodward/White, Aiken, SC. as well as in Chambers Global, Gaming 2008 and Chambers USA, Gaming and Licensing 2007.

Bradley J. Preber, Grant Thornton LLP, co-author
Bradley J. Preber is the managing partner of the Phoenix and Albuquerque offices of Grant Thornton LLP and is a partner in the Advisory Services practice in Phoenix. He also acts as the National Practice Leader of Litigation Services and the West Region Leader of Forensics, Investigations and Litigation Services. Brad has more than twenty-five years of accounting industry experience serving as a litigation consultant, expert witness, forensic accountant and fraud investigator. He is a Certified Public Accountant (CPA), Certified in Financial Forensics (CFF) and a Certified Fraud Examiner (CFE).

CONTRIBUTING AUTHORS
Michael Freudenthal, Senior Manager, Grant Thornton LLP
Kelly Gentenaar, Senior Manager, Grant Thornton LLP
Meredith Jonas, Manager, Grant Thornton LLP
Glenn Light, Lewis and Roca LLP
William Olsen, Principal, Grant Thornton LLP
Karl Rutledge, Lewis and Roca LLP
Quinton Singleton, Lewis and Roca LLP
Richard Springsteen, formerly with Grant Thornton LLP
Chapter 1
SURVIVAL OF THE FITTEST:
GOING BEYOND COMPLIANCE

What is a gaming license worth? To a gaming company, the answer is simple: everything. Without a gaming license, the company’s ability to earn revenue is extinguished. Regulatory compliance programs are an “insurance policy” for the company’s future and the ability of certain companies to earn either licenses or franchises that could be directly tied to the company’s regulatory history. Companies with substandard compliance records could find themselves at a disadvantage when they attempt to secure rights in or licenses from new jurisdictions. After all, an excellent predictor of a company’s future compliance is its history. Moreover, a good compliance program can literally save the company from the industry’s version of the “death penalty”—the revocation of the company’s gaming license after a disciplinary action.

Still, preservation should not be the sole motivating factor. To put it simply, good compliance is good business. Companies that are ethically run have a better reputation in the community and the industry. Within a company, strong compliance establishes both a corporate culture and a system of ethical behavior. Those that operate both ethically and legally can save much of the costs and ramifications of litigation and adverse governmental action. Further, the processes involved in compliance, including due diligence regarding prospective employees, business associates and others, can often supply information that is of valuable assistance in assessing the business risks associated with a particular hire or deal.

The false notion that compliance is the responsibility of the regulators is simply not feasible. Regulators have the expertise to define compliance goals and expectations of the companies either through regulation or review of the compliance plan; however, they do not have the resources, institutional knowledge of the internal workings of each corporation, or access to the corporate infrastructure that is required to effectively implement the compliance program. The idea of a compliance program is simple: it is an internal program adopted by a gaming company to ensure
compliance with all laws and regulations. For gaming companies, the program will have a particular emphasis on gaming laws, regulations and general regulatory policies. Successful compliance plans embody the commitment of the company to regulatory and legal compliance and focus on preventing regulatory violations. They identify areas of concern that might adversely affect the good reputation of the licensee. They also minimize the risk of being the subject of criminal or regulatory action and maintain the company’s reputation and goodwill. In the unfortunate circumstance where a company does find itself faced with criminal or regulatory problems, demonstration of a compliance program and a commitment to that plan can serve as a mitigating factor.

Regrettably, many gaming companies’ senior staff and boards of directors have little knowledge of the compliance function and therefore lack a commitment to the compliance process. Often, upper management relies on persons under them to understand the basic objectives of the gaming laws and how they apply to their business. The resulting decisions are based on what upper management may perceive as “acceptable” or “standard” in the industry.

This publication lays out the basic tenets of gaming compliance, including personnel requirements, attributes of an effective compliance plan, proper implementation and internal audits. Beyond the basics or regulatory minimums, this publication provides suggested areas where a company may effectively expand its compliance programs to work as preventive tools to avoid legal and regulatory issues and reinforce the company’s values on certain ethical and social issues. Such issues include campaign contributions, advertising and marketing policies, conflicts of interests, business ethics, securities issues, including insider trading and false or misleading disclosure and anti-trust issues, such as price fixing and concerted refusals to deal.
Chapter 2
WINNING PRINCIPLES: A SUCCESSFUL COMPLIANCE PLAN

Gaming compliance plans are as unique as the companies they protect. These plans are designed to identify and evaluate risks arising in the course of business that may negatively affect objectives to ensure sound and appropriate gaming control. Moreover, the nature and source of these risks and the ways they are identified and evaluated are particular to each company. Nevertheless, all effective compliance plans share certain attributes, such as a sound compliance policy and clear lines of authority and reporting.

Mandatory Requirements and Company Goals

The starting place for an effective compliance plan is well-reasoned and committed company compliance goals. Written policies should outline the reason for and the overall objectives of the compliance plan, together with the specific purposes of each of the policies. Typically, these policies reinforce the overall objectives of regulatory control, including that licensed gaming is to be conducted honestly and competitively, free from criminal and corruptive elements.

Mandatory Provisions

While some policies branch out to cover compliance with a variety of laws, such as election laws and corrupt practices, in the context of gaming regulation, the major goal is the timely identification and exclusion of unsuitable persons from gaming activities and the prevention, or prompt detection and correction, of unacceptable situations. Minimal requirements for implementation of this aspect of the gaming compliance are often set by gaming regulators or by regulation. See Box 1.

Although the contents of each compliance program will differ based on the size of the company and the nature of its operations, certain due diligence procedures are standard within every compliance program. These safeguards ensure that the licensee does not associate with unsuitable persons who
Getting in the Game: A Guide to Successful Gaming Compliance

might otherwise tarnish the company’s reputation. Such procedures include investigating and reviewing:

- Certain consultants, lobbyists, suppliers, vendors, distributors, advisors, lessees and tenants.
- Prospective officers, directors and key employees for past criminal and regulatory transgressions, past violations of corporate compliance plans and any misleading or false information of application.
- All material financings, such as significant debt or equity.
- Material transactions, such as joint ventures and partnerships.
- Major acquisitions or other strategic alliances.
- Any material litigation against the company or its employees.

The definitions of an **unsuitable person** and an **unacceptable situation** are helpful in focusing policies to meet company objectives

An **unsuitable person** is typically someone who the gaming authorities or company officials determine to be unfit to be associated with a gaming licensee. This may be a subjective decision, for example, barring an individual notorious for unsavory personal conduct or affairs. In certain circumstances, suitability may be determined more objectively based on a prior denial of a gaming license, other regulatory approvals, or on felony convictions involving moral turpitude, gaming law, narcotics law, or any criminal-related activities.

An **unacceptable situation** is any event or circumstance that may adversely affect the objectives of gaming control by diminishing the public faith in the ability of the gaming authorities to assure the honesty of the games and the integrity of the industry. Both objective and subjective criteria should be set forth in the compliance policies to identify unsuitable persons and situations.
Discretionary Goals

More sophisticated compliance plans will create methodologies to use the compliance process to help ensure regulatory compliance with laws other than gaming laws. These plans may incorporate policies and procedures for securing compliance with among other things: (1) securities issues, including insider trading and false or misleading disclosure; (2) Bank Secrecy Act and anti-money laundering; (3) campaign contribution laws; (4) Foreign Corrupt Practices Act; (5) anti-trust issues; (6) advertising and marketing policies; (7) conflicts of interests; and (8) the Patriot Act. The plan can be used not
only to educate and guide company employees in these important areas, but also to create a reporting mechanism that helps avoid potential issues and enforcement mechanisms to discover and remedy problems. Each of these areas is discussed in greater depth in this publication.

The program should be in a written format and should explain how the company will implement the plan. It should begin with a general statement of the corporate policy and then go into detail about the strengths and weaknesses of the existing company infrastructure, any specific compliance issues or problems, and the like. The program should be continually updated to meet new regulatory requirements, changing environments and new regulatory challenges and problems.

Box 2

Typical Compliance Plan Provision Dealing with Vetting Officers, Directors and Key Employees

The Parent Company and its Subsidiaries shall exercise care to ensure that prospective Directors, Executive Officers and Key Gaming Employees of any Gaming Subsidiary, and Directors and Executive Officers of the Company are not Unsuitable Persons. The suitability of prospective Directors, Executive Officers and Key Gaming Employees shall be investigated and the results reviewed at the direction of the Compliance Officer. The results of such investigation, should any derogatory information be revealed, shall be reported to the Compliance Committee for review and appropriate action.
Chapter 3
THE KEY PLAYERS IN THE COMPLIANCE GAME

Once a gaming company knows what it wants to accomplish, it needs to determine how to accomplish it. Ultimately, all officers, directors and employees of a company and the regulators are involved in the compliance process, but the responsibility of any effective compliance program falls on the compliance committee, the compliance officer and the board of directors. The compliance plan needs to create and delegate clear authority to each group.

The Compliance Officer: The Heart of the Program

The compliance officer is responsible for overseeing the implementation and administration of the company’s compliance programs and internal reporting system. The compliance officer has multiple responsibilities, including:

• Interacting with the various corporate divisions to determine situations requiring reporting under the internal reporting system and review by the compliance committee.

• Conducting and coordinating mandatory background investigations of all areas for which the compliance plan requires mandatory review - including prospective management and key employee hiring, review of suppliers and vendors, and material litigation.

• In-taking and coordinating review and investigations of business practices that may constitute an unsuitable method of operation, employee reported violations, criminal investigations of or involving the company or management, and the like.

• Documenting all activities and preparing all reports for the compliance committee as required by the compliance plan or otherwise helpful in the compliance process.

The compliance officer must have a proper background. Familiarity with the laws that govern gaming operations and an understanding of the expectation of the gaming regulators regarding the proper conduct of
a gaming licensee are essential. The compliance officer must be familiar with the company’s corporate structure, including the functions of parent, affiliate and subsidiary companies, and must possess the administrative skills to coordinate compliance across the various company departments. He or she must have the ability to conduct employee training, document all compliance activities and functions, and coordinate internal investigations.

The compliance officer must receive sufficient training and be adequately remunerated for his or her services. He or she must be provided with the necessary resources required to conduct his or her job and to ensure inter-departmental and management co-operation exists in regard to the compliance program. The compliance officer should be brought in early on all potential transactions. This allows all necessary due diligence reviews to be conducted before transactions are finalized.

**Compliance Committee**

Members of the compliance committee should be individuals who, by virtue of their familiarity with the law and the business activities of the company, are sensitive to the concerns of the gaming authorities and are capable of determining the existence or likelihood of an unsuitable situation that could

---

**Box 3**

**Typical Compliance Plan Provision Dealing with Composition of Compliance Committee**

*The compliance committee shall be comprised of at least three (3) members and not more than five (5) members. The membership of the compliance committee shall include the Chief Financial Officer and the President of the company. The membership of the compliance committee also shall include at least one person experienced in the gaming regulatory process who is familiar with the laws governing gaming activities in the jurisdictions where the company conducts business and who is a person independent of the company. The members of the compliance committee should be individuals who, by virtue of their familiarity with law enforcement, regulated businesses, the business activities of the company or gaming control, are sensitive to the concerns of the gaming authorities and capable of determining the existence or likelihood of an unsuitable situation.*
adversely affect the reputation of the gaming company. The committee must understand the gaming business and the regulatory process and objectives. The committee needs to have the cognitive ability to assess situations and proffer recommendations that meet regulatory objectives and will have the least adverse impact on business operations.

The compliance committee, acting through and with the assistance of the compliance officer, generally is empowered to investigate, evaluate, report facts, and make recommendations of possible responses or initiatives for senior management’s considerations, including disciplinary action related to misconduct by company employees or agents.

The compliance committee generally consists of three to five members, typically including the chief financial officer, the president, and at least one outside person. While some compliance committees have gravitated toward having more or all outside members to allow for greater independence, the value of having inside members—such as corporate officers—is a greater understanding of corporate structure, dynamics and culture that is invaluable to the committee’s work.

The members of the compliance committee are usually appointed by, and shall serve at the will and pleasure of, the company’s board of directors, subject to any required approvals of the gaming authorities.

The compliance program should delineate the procedures that the company will employ in selecting and appointing the committee, as well as the procedures that govern the duties and responsibilities of the compliance committee.

**Board of Directors**

The board of directors is responsible for appointing the compliance officer and supervising the compliance committee. All reports generated by the committee through the compliance officer should be submitted to the board of directors for approval by the chairman of the board. The board should have discretion to change, modify, or update the plan as it deems necessary. The board bears primary responsibility of the compliance plans
and the actions taken by management. The compliance plan will remain in effect until the compliance plan is rescinded by the board.

**Senior Management**

The overall responsibility to oversee compliance functions should be assigned to the senior management of the company. The organization’s culture starts at the top. The program should then create and delegate clear authority for each group within the compliance structure, including the compliance officer, the compliance committee, employees and the board of directors. Senior management has the primary responsibility for the implementation of the compliance plan. As such, senior management must properly fund the program, provide leadership in implementing and integrating the compliance plan, and be willing to evenly enforce the plan across all levels of the company.

**Company Employees**

The success of this reporting system also depends on the coordination and cooperation between the various departments within the company, such as corporate planning, development, acquisition, human resources, procurement, finance, legal, internal audit and sales, whose business functions may give rise to compliance review issues. Moreover, employees should be made aware of the importance of remaining vigilant and reporting violations. Gaming businesses should therefore include compliance behavior as an element of employee evaluation for promotion, bonus and salary decisions. Conversely, bad compliance behavior should result, when warranted, in disciplinary action.

**Gaming Authorities**

The gaming authorities play a key role in the success of a compliance program. Accordingly, the compliance officer, compliance committee, board of directors and senior management will all benefit from establishing a working relationship with the gaming authorities.

In Nevada, for example, the gaming regulators include the Nevada Gaming Commission, Nevada State Gaming Control Board and all other regulatory authorities having jurisdiction over the company’s gaming business. The
gaming regulators generally set the minimum standards for a compliance program, review and approve the program (after endorsement by the board of directors), and assist the company in the program’s implementation. All copies of minutes, reports, exhibits and documents relating to items considered by the compliance committee must be provided to the gaming regulators for review and recommendation.

Moreover, the gaming regulators are responsible for auditing the compliance program at the company. This periodic review is significant in ensuring the compliance program continues to remain effective after implementation.

The review will consider a number of questions, including: Are the compliance controls working? Do the compliance controls adequately detect the types of regulatory violations and crimes that the company is vulnerable to? Has the compliance program been modified or adapted to take into account any known criminal or regulatory violations? Should the compliance program be reviewed or updated to reflect any new company or industry threats or to reflect best practices within the industry?
Chapter 4

HOW TO MAKE YOUR PLAN FUNCTION

Underlying compliance policies are the methodologies for obtaining information regarding potentially unsuitable persons or situations. One source of information is a comprehensive set of internal reporting systems, including self-reporting by corporate officers and upper management. Effectively, these individuals should have a clear and defined affirmative obligation to report unsuitable situations, whether they are personal (such as being arrested) or involve business operations.

Another way to collect information on compliance is through whistleblower programs. These are programs that often involve a delineated system for anonymous reporting of unsuitable situations observed or suspected by company employees or others. Whistleblowers may be found inside and outside the company. Insiders include employees and directors. Outsiders may be vendors, regulators and investors.

In addition, information received from gaming regulators or other law enforcement entities regarding operational issues or relationships may be a good source for identifying compliance risks. This could include a written notice from gaming authorities concerning alleged wrongdoing, which could have an adverse effect on the objectives of gaming control or otherwise violate compliance policies.

The company also may automatically collect information on transactions or situations, such as material civil litigation, material transactions, major developments, material corporate financings, material contracts with major suppliers of goods and services, lease contracts, incidents reported in suspicious activity reports, and internal audit reports. Collected information should be limited to only material or major matters. For example, suppliers receiving more than $100,000 annually could be required to complete preprinted background forms. The plan should then specify what happens to the information once submitted. The compliance officer may have the responsibility to review the forms for completeness and to conduct other investigations to complete the information required for the compliance committee’s review.
Independent investigation of parties to a transaction may not be required in instances where the party under review is regulated by a governmental agency. For example, a compliance plan may permit a company to forgo an independent investigation of a publicly held company regulated by the Securities and Exchange Commission. This may extend to a financial institution regulated by federal banking authorities, a company or individual regulated or licensed by one of the gaming authorities, or a gaming regulatory authority of a foreign jurisdiction, other than to determine the other party’s standing with such governmental agency. Even compliance plans permitting a company to forgo an independent investigation usually contain a caveat that if any reason exists to believe that the company may be unsuitable, then an independent investigation still may be warranted.

The nature of the information that the compliance officer collects and reports to the compliance committee varies depending on the transaction.

In the case of material financing, this information typically includes:

- Source of the funds.
- Disclosure of any relationship among the company, any subsidiary and any other parties to the proposed financing.
- Identifying any finder, broker, or other person who is to receive compensation in connection with securing, arranging, negotiating or otherwise dealing with the proposed material financing.

In cases where the funds are not from institutional lenders, the compliance officer may conduct due diligence on the lender.

Material transactions are typically defined by reference to thresholds appropriate to the size of the gaming business. In regards to material transactions, the reports shall typically include the following information with respect to the other party to the transaction; to the extent such information is known by the compliance officer.

- Name and address.
- Legal form, such as corporation, partnership, or joint venture.
- Nature of business conducted.
Box 4

Typical Compliance Plan Provision Defining a Material Transaction

Material Transaction means a transaction whereby the compliance officer or a member of the compliance committee has knowledge that pertains to:

A. A commercial transaction involving an unsuitable person or an entity that reasonably may be regarded as an unsuitable person

B. The acquisition or disposition of assets or equity interests where the value given or received by the company or a subsidiary exceeds three million dollars ($3,000,000) or five hundred thousand dollars ($500,000) if solely related to the company, except for such transactions involving temporary investments in securities as included on the company’s consolidated balance sheets or the purchase or disposition of less than 20 percent interest in a non-gaming entity or facility.

• Geographical area where business is conducted.
• Names and addresses of all directors, principal officers, shareholders holding more than five (5) percent interest, general partners and any limited partners holding more than five (5) percent interest.
• Brief statement as to the company’s reasons for the proposed transaction.
• Specific laws under which the business operation is permitted, if relevant.
• Identification of any person such as a broker or finder who is to receive any form of compensation for suggesting, proposing or arranging the transaction, including the arrangement for such compensation.

Reports of all gaming equipment sales or leases by geographical area shall be maintained. The reports should contain the following information:

• Name and address of the purchaser/lessor.
• Description of machines.
• The jurisdiction into which machines are to be shipped.
• Identification of any broker or finder involved and compensation arrangements.

An internal reporting system is also typically established as part of the gaming compliance and reporting program. The system is designed to detect any criminal conduct by the company’s employees or other agents and requires the licensee to immediately report to the gaming authorities any and all violations of the compliance plan. Self reporting demonstrates to employees, prosecutors and investigators that the provider is committed to building a culture of compliance. Furthermore, federal sentencing guidelines require the company to have in place, and publicize, a reporting system whereby employees and agents can report criminal conduct by others within the organization without fear of retribution.

Regardless of the source of the information, the compliance plan should provide standardized directions for the compliance officer to conduct any investigation necessary to assist the compliance committee to reach conclusions about allegations.

The compliance committee efforts should be focused on reviewing information and reports developed by the compliance officer and determining a proper course of action. They should be afforded the cooperation of company personnel, including security, surveillance, and internal audit to accomplish the company’s compliance objectives. In addition, the compliance committee should have the authority and financial resources to hire outside expertise, if necessary, to conduct a complete and comprehensive investigation.

All compliance committee activities, except for certain investigative actions, should be transparent to company directors, top management and to gaming regulators. This can be accomplished by disciplined record keeping and reporting. The compliance plan should prescribe record production, maintenance and retention requirements. This should include original complaints, police reports, employment applications, as well as records of investigations and other materials. Finally, the compliance committee should maintain detailed minutes of meetings and decisions.
The committee will usually meet at least quarterly to review reports and other information provided by the compliance officer. The committee is expected to digest and act upon source materials, such as the original complaints, police reports, employment applications, independent material such as background investigations, detailed minutes of past committee hearings, including compliance-related decisions and decisions as to why an investigation was terminated, and the report of the compliance officer. The committee is expected to make specific and clear recommendations to management on how to handle particular circumstances—from hiring and firing decisions to the acceptability of entering certain gaming markets. The committee will prepare and submit to the board of directors, or an equivalent body designed by the compliance plan, a periodical report summarizing its activities and decisions.

**Authority and Reporting**

To function well, a gaming compliance plan requires structure and a clear delegation of authority and reporting. In most companies, major responsibilities for monitoring and ensuring compliance fall on a specially appointed compliance committee. The compliance committee helps the company comply with gaming regulations and other laws. The committee’s primary purpose is to identify and properly investigate potential violations of gaming statutes and policies, and to formulate recommendations on a course of action that the company may consider in appropriately addressing specific transactions or situations based on the collected materials and collective experience. Ultimately, the company, not the compliance committee, has responsibility to determine the course of action related to unsuitable persons or unsuitable situations and to interface with the regulators.

The composition of the compliance committee, including the number of members, qualifications, and division of duties between internal staff members (officers and employees) and outside members, should be described within the compliance plan. Historically, compliance committees have consisted of the company president, a chief financial officer and one or more independent members. These independent members are typically selected based on their familiarity and experience with law enforcement,
regulated businesses, the business activities of the company or gaming control. They are expected to be sensitive to the concerns of gaming authorities and capable of determining the compliance with gaming statutes and company compliance policies.

In addition, the compliance plan should delineate how compliance committee members are to be appointed and how changes may be made. In many jurisdictions, the company may be required to report or obtain approval for changes in compliance committee membership. If so, this should be reflected in the compliance plan. The plan should also cover administrative matters like the frequency of meetings, definition of a quorum, and compensation.

Company policies and the compliance committee represent two key aspects of an effective compliance plan. Another is the use of a corporate compliance officer as the key liaison between the company and the compliance committee. The compliance officer is responsible for coordinating, monitoring, testing and reporting company compliance efforts. The compliance officer has the responsibility for collecting necessary information needed by the compliance committee to make informed decisions.

To avoid confusion and possible duplication of efforts, the compliance plan must provide a description of duties, responsibilities, authority, and lines

---

**Box 5**

**Typical Compliance Plan Provision Dealing with Reporting Detail by Compliance Officer**

Reports to the compliance committee and the minutes of meetings of the compliance committee shall contain that detail necessary and appropriate to permit a well-reasoned decision by the compliance committee member on each subject considered by the compliance committee. Except in circumstances indicating that reliance is unreasonable or unwarranted, independent investigation is not required with respect to information that is widely disseminated or otherwise a matter of public knowledge, and such information may be excluded as the subject of a compliance committee report unless the information relates directly to an issue to be considered by the compliance committee.
of reporting for the compliance officer, the compliance committee, senior
management, company employees, and the board of directors. Typically,
the compliance committee will report to the board of directors and the
compliance officer will report to management. If designed correctly, the
compliance plan is a management tool, with each key player serving a distinct
and appropriate role. However, compliance plans may fail by not properly
defining these functions and responsibilities. A compliance officer that
believes he or she has the obligation to collect, judge and report situations
to regulators outside the compliance process will soon lose the faith of
the company and the compliance committee. Moreover, regulators could
receive raw information without the informed review by the compliance
committee, whose input is vital.

Gaming regulators may ask to review (1) the proceedings and
recommendations of the compliance committee, (2) the due diligence
of the compliance officer in collecting and presenting information, (3)
the sufficiency of the company’s consideration of compliance issues and
response to committee recommendations, and (4) the accurate reporting
of situations to the authorities. This inquiry is conducted within the confines
of the delegated authority set forth in the compliance plan.

As noted earlier, no two compliance plans are alike, just as no two gaming
companies are alike, and to be effective, each plan must reflect the individual
nature of the company it serves. However, to be truly effective, compliance
plans must meet the fundamental requirements outlined here.

Compliance is a duty of all gaming companies. This commitment starts with
prioritization of compliance among the company’s objectives. The company
should proceed by undertaking an assessment of its infrastructure and
organization to understand current capabilities. Where regulatory voids
exist, they need to be addressed in the compliance structure. The company
also needs to survey its current business activities and past compliance
history to detect potential problem areas. Past compliance issues may
require special assessment of the needs to be considered in investigation,
monitoring or reporting. Often a good place to start is to consider past
disciplinary proceedings or issues that may have arisen during the course of
the licensing investigation.
The company also should survey compliance programs and successes within the industry. While much of the substance of a compliance plan may be derived from regulatory requirements or review, the better compliance programs are proactive as opposed to reactive. A review of disciplinary issues faced by other gaming companies may suggest the need for additional diligence in those areas.

Compliance should be implemented through employee training, program monitoring and enforcement. The methods of communication may differ depending on the size of the company. Compliance should not be seen as a “one size fits all” concept. Smaller companies may effectively communicate requirements informally, while larger companies may need to formalize the method of communication. Methods of communication may include the orientation of new employees, employee newsletters, pay stubs, messages, posters, public recognition for ethical behavior and ethical review in performance evaluations, and promotion considerations. Employees also should be provided with disseminating publications that explain, in a practical manner, what is required, as well as provide the name and contact number of the compliance officer.

The compliance program should account for each role within the company and the separate duties and responsibilities they entail. For instance, cashiers need instruction on certain subjects, casino hosts on others, while accounting reviewers need a different type of training. Moreover, compliance should not be seen as a one time event. A constant review of industry practices may assist in augmenting an existing compliance plan. Training courses should occur on a periodic basis to refresh the understanding of compliance fundamentals, introduce changes in gaming laws and regulations, and address the impact of the compliance program, and any emerging issues resulting from it.

The policies also should set out the responsibilities of officers, directors and employees. They should mandate adherence to the compliance plan and state the consequences for non-compliance. Penalties for violations may include prosecution, demotion, and summary termination of employment. Communication, education and training are a key component of success.
As with any critical company objective, gaming management and officials should lead by example by fully complying with the policies to set the proper tone “at the top.”

**Box 6**

**Typical Compliance Plan Provision Dealing with Minutes of the Compliance Committee**

The compliance committee shall prepare and maintain minutes recording the business considered and decisions rendered by the compliance committee at each meeting. Copies of the minutes of the committee meetings shall be provided within ten (10) days after ratification by the compliance committee to the Regulatory Committee, all compliance committee members, and concurrently to the Chairman of the Gaming Control Board, along with copies of all documents, reports and exhibits submitted to the compliance committee by the compliance officer. The minutes shall identify all matters considered by the compliance committee and shall contain the amount of detail appropriate to permit a well-reasoned decision by the compliance committee members. In those matters in which the compliance committee takes no action, the minutes shall reflect the reasons why no action was deemed appropriate.
Chapter 5
WHISTLEBLOWER PROCESS AND SARBANES-OXLEY ACT REQUIREMENTS

The Sarbanes-Oxley Act of 2002 (SOX) formalized the importance of whistleblower programs for U.S. publicly-held companies, including public gaming enterprises. Audit committees of these companies are especially impacted as they are charged with “establishing procedures for (a) the receipt, retention and treatment of complaints received by the issuer regarding accounting, internal accounting controls or auditing matters, and (b) the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters.” (SOX § 301, Public Company Audit Committees, Title III)

Unfortunately, Congress provided no guidance to audit committees on the types of procedures to be used or how to evaluate the effectiveness of whistleblower programs once established. Therefore, for many public gaming companies, complaint handling is an undisciplined process that seems to operate as if every matter is a crisis. It can be inefficient, expensive and lengthy, yielding few, if any, measurable results.

Many companies fail to recognize the vital role whistleblower complaint handling plays in deterring and preventing corporate fraud. In fact, controls that prevent, deter or detect and correct fraud are critical: after all, the best case scenario is a fraud that never happens. This is reflected in the Association of Certified Fraud Examiners’ (ACFE’s) 2008 Report to the Nation on Occupational Fraud and Abuse (“ACFE Report,” www.acfe.com).

In the ACFE Report, a study of 959 cases of occupational fraud shows that the initial detection of fraud usually is not the result of internal controls alone. Instead, tips, most often from employees, are the most common source for fraud detection in the workplace.

Requirements

The SOX requirements regarding whistleblower programs are clear—public gaming companies must have effective processes that guarantee complaints are heard and dealt with properly. Procedures built into the
process must “facilitate disclosures, encourage proper individual conduct and alert the audit committee to potential problems before they have serious consequences” (SOX § 301, Public Company Audit Committees, Title III).

In summary, the SOX requirements are to:

- **Facilitate disclosures** by discovering, in a timely manner, evidence of activities that may threaten or impede compliance with laws, rules, regulations and standards related to financial statements and associated disclosures, regulatory filings, and other public disclosures.

- **Encourage proper individual conduct** by providing a process that, when implemented and properly maintained, will assist in efforts to reinforce pre-defined and acceptable ethical behaviors related to accounting, internal accounting controls or auditing matters or, alternatively, will prevent or detect and correct unacceptable conduct.

- **Alert the audit committee, or other governing body, to potential problems before they have serious consequences** by establishing an “early warning system” to bring accounting, internal accounting control and auditing matters to the attention of the audit committee in time to prevent, or detect and correct, possible problems before they cause serious harm or damage.

To meet these responsibilities, directors and management must ensure that the public gaming company implements and monitors an appropriate process and procedure for dealing with whistleblower complaints swiftly, cost effectively, and efficiently in connection with accounting, internal controls over financial reporting, and auditing matters.

**Users**

Initially, it is essential to identify the potential users of the complaint handling program and to understand their often disparate needs. There are three primary groups of users, as follows:
• **Whistleblowers** are the persons who file complaints. These parties can be internal, such as employees, management or directors, or external, for example, customers, vendors, or investors.

• **Accused parties** are individuals, groups (e.g., department) or companies that are the focus of the whistleblower complaint. These parties may also be internal or external to the company.

• **Other interested parties** are those with a vested interest in the asserted claim, investigation and/or its outcome. Within the company, these parties may include the general legal counsel, internal audit, risk management, information processing, human resources or public/investor relations. Outside parties with an interest might be external legal counsel, lenders, regulators, insurers and independent auditors.

Anyone with a concern about accounting, controls or auditing matters should feel comfortable using the complaint-handling program. This is especially true for internal users who may fear that filing a complaint will cost them their job or cause some other adverse effect. The usefulness of a whistleblower complaint-handling program can be enhanced when it has the following attributes:

• **Choice of reporting venues**—In a well-designed program, complaints can be submitted through discussions with supervisors, confidential conversations with human resource personnel, anonymous “tip” lines, company Web sites and e-mail.

• **Confidentiality and anonymity**—This is a must. In fact, SOX requires that audit committees establish procedures for “the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting controls or auditing matters” (§ 301 of SOX, note that customers and vendors as anonymous sources are not contemplated).

• **Ease of use**—Many users want simply to pick up a phone or send an e-mail to make a complaint. Experience shows that users avoid programs with layers of bureaucracy.
• **Information on progress of complaint**—Reporting and feedback mechanisms should be sensitive to context. On one hand, whistleblowers want to know that claims are handled expeditiously and that the company is addressing the concern. Conversely, for sensitive complaints, it is important to protect the gaming company and its management, the accused party, and others potentially impacted by the complaint. In such cases, progress reports may not be appropriate.

To demonstrate the credibility and objectivity of the program, it is important to emphasize that the audit committee has sole responsibility for the receipt, handling and investigation of accounting, internal control, and auditing matters. Further, employees should be assured that legal counsel will be used to protect them and the company. Users will also gain confidence in the process if they are aware that investigations will include consultation with qualified advisors, both internal and external to the company.

**Program Steps**

An effective whistleblower complaint handling program has six basic steps:

1. **Receive** the complaint.

The act of receiving a complaint requires training and a disciplined method for documenting and filing claims. Every whistleblower claim, whether delivered in person or by written means, should be logged, tracked, and controlled. This also helps to preserve whistleblower anonymity.

Any claim with the potential to significantly impact the gaming company’s financial statements is the responsibility of the audit committee. However, if every claim is brought to the audit committee for handling, they would quickly be overwhelmed. Therefore, it is recommended that the receipt of each claim include a screening for relevance and importance. Such a screening can be performed by a committee, with its members overseen by the audit committee. Alternatively, these duties may be delegated to an adequately trained and qualified outside service provider or consultant. Screeners should have access to company management and personnel to conduct the initial analysis of the claim.
The screening process is designed to determine the merit and relevance about the claim:

- **Merit**—Is the claim credible, valid and substantiated? If so, it should be referred to the appropriate company governing body for further analysis. Any claim that has merit must be referred for possible investigation.

- **Relevance**—Is the claim related to accounting, internal accounting controls or auditing matters? If the answer is yes, and if the claim has merit, it will be referred to the audit committee for further analysis and possible investigation.

At this early stage, any interaction with personnel should be restricted, deemed confidential, and remain anonymous. Any requests for documents and interviews should be coordinated with company legal counsel. The decision on whether or not to investigate a whistleblower claim is based on the available facts and circumstances. Frivolous complaints are often made and disgruntled employees may want to inappropriately express concerns through the claims handling program. In addition, complaints may not be related to fraudulent activity, accounting, and auditing matters.

2. **Analyze** the complaint.

After the audit committee receives a whistleblower complaint from the screeners, it should perform additional analysis, assisted by company legal counsel, to discover relevant facts and information and determine a course of action. This is made easier by using standards for identifying and handling complaints. The use of standards assures objectivity, allows the audit committee to quickly identify any advisors that may be needed, and improves the efficiency of decision-making. Following are the two main standards the audit committee must consider:

- **Sensitivity**—Facts and circumstances that, if disclosed, may cause significant harm to the gaming company. Examples may include the alleged involvement of a senior officer or director, violations of law, and a breach of fiduciary duties, among others.
• **Materiality**—Situations that have the potential to significantly impact the reporting and disclosures of the financial statements, regulatory filings, restrictive covenants or incentive compensation, along with other matters.

The audit committee determination of sensitivity and materiality for a claim requires consideration of qualitative (i.e., adverse impact) and quantitative (e.g., monetary amount) matters.

3. **Investigate** the complaint.

The manner in which a whistleblower complaint is investigated depends on its sensitivity and materiality, as determined by the audit committee. If a complaint is deemed to be neither sensitive nor material, the investigation can be assigned by the audit committee to disinterested management personnel and employees of the company. However, for any other claim, the audit committee should consider the potential risk for an actual or perceived conflict of interest from using internal personnel to perform the investigation. At a minimum, the audit committee should engage independent, external legal counsel to oversee and supervise the investigation. In the case of sensitive but non-material complaints, the audit committee will want to carefully consider whether certain internal groups need to be involved at all. Depending on the situation, the audit committee may also want to bring in external advisors such as forensic accountants, specialty attorneys (e.g., regulatory, employment, insurance), bankers, insurance experts and credit specialists to assist with an investigation.

4. **Resolve** the complaint.

At times, resolving a complaint impacts only a small part of the company, as in the case of the handling of a single invoice or an expense report. Conversely, such steps as the termination of a senior executive officer for indiscretions or the restatement of previously issued financial statements are likely to be serious and far-reaching. Accordingly, resolving a complaint requires the diligent and focused efforts of the audit committee to design and implement appropriate corrective actions.
A corrective action plan, or remediation plan, establishes procedures to be performed and actions to be taken to address a whistleblower complaint. A remediation plan may call for the improvement of an internal control, the delivery of training, a financial statement restatement, or a personnel action. Any remedial plan must be approved by the audit committee. Before adoption, the audit committee typically will consult with management and external advisors to understand company resource requirements, the level of effort, costs, and limitations of adopting the resolution.

The audit committee should monitor each remediation. Any material changes to the plan should be reviewed and approved by the audit committee. After completion, the claim under investigation is closed, reported and retained as described below.

5. **Report** the resolution of the complaint.

Actions taken in connection with a complaint will generate curiosity and be closely watched by the whistleblower, the accused and other interested parties. Whistleblowers will expect timely reports on the status. Innocent suspects want their innocence to be communicated promptly. Guilty parties must be dealt with swiftly and decisively. The company’s responsiveness signals that it takes complaints seriously and is prepared to deal with them appropriately. As such, it is critical to have defined communication and reporting protocols in place.

Communication and reporting protocols must consider confidentiality and provide a reasonable level of disclosure to all interested parties. Management, directors, shareholders, and employees have differing needs and requirements than regulators, auditors, and creditors. The preparation of a communication and reporting protocol and the content and delivery of information may require the assistance of legal counsel, public relations professionals, and others to reduce any risk related to incomplete or inaccurate disclosures. In addition, because of anonymity requirements, documents and reports must be safely secured, the chain of custody maintained, and the distribution and use properly restricted.
6. **Retain** the necessary documentation.

Documents produced from the whistleblower complaint handling program, and any associated analysis and investigation, should be retained in accordance with the company’s document retention policies. Complaints filed, in compliance with SOX, are confidential matters requiring anonymity to the whistleblowers under the law. Therefore, it is important to restrict access to documents and to protect electronic data. These records and data also serve as evidence of the audit committee’s compliance with SOX and as proof that the company successfully addressed any accounting, internal control, and auditing risks.

**Monitoring and Metrics**

As with any system, the whistleblower complaint handling program must be monitored and tested for compliance with the objectives and metrics established by the audit committee. Monitoring can be performed by the company’s internal auditors or by outsourcing to a contractor.

Metrics to measure the effectiveness of the program empower the audit committee to know whether the whistleblower complaint handling program is a success. Metrics point to areas that need improvement and allow for trend comparisons across the organization and against industry standards.

**Maintaining SOX Compliance**

SOX requires that audit committees meet expanded responsibilities using procedures to handle whistleblower complaints about accounting, internal accounting controls, and auditing. Handling serious whistleblower events is hard to prepare for—yet one misstep can have devastating effects. Companies and audit committees need to have an effective plan and process in place before whistleblower events arise. This means that a systematic program is needed to effectively perform these procedures. An effective whistleblower program is designed to meet unique user needs and follows a disciplined process to receive, analyze, investigate, resolve, report, and retain incoming claims.
Chapter 6
INTERNAL INVESTIGATIONS:
LACK OF A PLAN CAN BE RISKY

The decision to begin a gaming investigation is important: in fact, it may be critical to keeping a gaming company’s most valuable asset its gaming license. Efforts to discover potential compliance violations and the timing and diligence of an investigation can show regulators and others that the gaming licensee can effectively identify and respond to allegations of wrongdoing. More importantly, a thorough and objective investigation shows the gaming enterprise’s commitment to comply with all governing laws and regulations. Together, a proactive issue discovery process and the prompt, objective and comprehensive investigation of compliance issues demonstrate that the gaming company can self-regulate without undue outside intervention.

Issue Discovery

The process used to discover potential compliance violations is an important part of a credible and effective compliance program. A gaming enterprise must establish methods and procedures and provide the necessary resources to actively seek information about potential problems. This is best accomplished through a clear set of written and communicated polices that define acceptable behavior and practices.

Whistleblower complaints are common ways to find potential fraud or to become aware of compliance violations. Regulators and stakeholders expect gaming companies to establish and maintain a system to effectively receive and deal with whistleblower complaints. Creating a process designed to properly receive and screen complaints, analyze claims, investigate and resolve any issues, report the results, and retain essential documents is the best way to handle whistleblower complaints.

Whistleblowers

The first step to establishing an effective whistleblower complaint-handling system is to identify possible users and understand their needs. Employees, management or directors of the gaming operation are potential users. These individuals can be the whistleblowers or the targets of complaints.
Additionally, customers, vendors, suppliers, or investors from outside the gaming company also may generate complaints.

Once potential users are identified, understanding each user group’s unique, and often disparate, needs is critical. To do this, management should determine user awareness of any existing complaint handling process. Knowing how and when the process has been used in the past, or might be used in the future, is important. For example, users may be most comfortable reporting suspicions directly to supervisors, through telephone hotlines, or using e-mail. In general, user preferences relate to a choice of methods to report problems, a need for confidentiality and anonymity, ease of use or convenience, and a desire to access information on the progress of their complaint. The whistleblower complaint handling system will not be fully functional if users perceive that barriers exist that prevent using it, or if it fails to effectively meet their perceived needs. A busy tip hot-line, a breach of confidentiality and/or an unanswered e-mail can cause the process to fail. Therefore, potential obstacles should be identified and removed.

**Receiving a Complaint**

The act of receiving a complaint may seem like a simple task. You listen to a problem and work to find a solution. Receiving a whistleblower complaint, however, is more complicated. To ensure all complaints are captured and reported to the appropriate level of management, a standardized method should exist for employees to accept and document concerns. This requires that employees are trained to intake and document claims.

Each complaint, whether spoken or written, should be documented, reported, and tracked to ensure proper and timely resolution. Information critical to understanding and investigating a complaint like documents and files, should be obtained from whistleblowers and secured. This simple step can save valuable time, costs, and effort later on in an investigation. If the whistleblower is an employee, a promise of anonymity must be honored as required by federal and state laws.
Investigative Analysis

After accepting a complaint, gaming companies face the challenge of determining whether to pursue a specific matter based on available facts. Therefore, properly screening complaints is crucial. Frivolous complaints are common, and disgruntled employees may use the whistleblower process to vent frustrations or sabotage management. Others may use it to make harmless suggestions to improve company operations. Therefore, company officials need a process to screen complaints to sort out “red herrings” or “false positives” from substantive concerns. In other words, gaming companies need a reliable way to separate real issues requiring urgent responses from those that can be safely ignored or classified as lower priority.

One suggested method to use is to sort complaints into classes based on two criteria—sensitivity and materiality. Sensitivity rates claims on the basis that, if disclosed, they may cause significant harm to the company. They might include allegations involving senior ranking officials and violations of gaming and other laws. Materiality relates to matters that have the potential to significantly affect financial statements, regulatory filings, restrictive covenants or incentive-based compensation. Both require an analysis of qualitative (i.e., potential adverse consequences) and quantitative (e.g., dollar amounts) factors.

Conducting the Investigation

How a whistleblower complaint is investigated depends on its sensitivity and materiality. Specifically, the attributes of the complaint determine which groups within and outside the gaming operation will need to be involved. For publicly-owned gaming companies, federal law requires that matters directly concerning financial reporting and internal accounting controls will fall under the responsibility of the audit committee, which is an operating committee of the board of directors, that oversees financial reporting and disclosure. If a complaint is neither sensitive nor material, the compliance officer, a disinterested member of management or the internal audit group can conduct the investigation.
Depending on the situation, gaming companies may engage independent advisors to avoid any appearance of a conflict of interest or to supplement internal resources with specialty skills. For example, whistleblower investigations often require the use of forensic accountants, specialized legal counsel (such as regulatory, labor and employment, insurance), and credit advisors. Identifying, qualifying, and contracting for expertise should be done in the planning phase of the whistleblower complaint handling process, before an actual whistleblower event occurs, to ensure that resources are available when needed at reasonable cost.

Before beginning an investigation, the company should set a clear definition of success and an understanding of the time and resources needed to achieve it. Success may include prosecution of a suspected criminal, recovery of lost assets, preparing a proof of claim under insurance coverage, or the strengthening of a weak internal control system. Such objectives should be shared with the investigation team and used to measure progress and issue resolution.

Gaming companies also should evaluate the impact the investigation may have on key stakeholders inside and outside the organization. The whistleblower will want to know what is happening with the complaint and the implicated individuals will need information to defend themselves. Others, such as regulators, investors, external auditors and lenders, also may have a stake. External auditors may even want to shadow the company’s investigation. Everyone may be curious about the possible effects of the investigation on their interests. Of course, an investigation never goes exactly as planned, so consideration of possible adverse consequences, such as counterclaims and regulatory inquiries, is important.

A complete and comprehensive investigation will consist of all necessary procedures and actions to provide for the discovery, location, and recovery of sufficient facts to reach an accurate and defensible conclusion. This will often require the use of forensic specialists to identify, analyze, and preserve evidence, particularly in connection with mass quantities of electronic data prevalent in gaming operations. In connection with this, the investigation team must determine who should receive sensitive information as it becomes
available. A plan to handle information leaks and rumors that will inevitably occur during the course of the investigation should exist. In certain cases, involving public and investor relations personnel may assist in the design and delivery of an effective communication plan. In any case, legal counsel should advise the company on who needs to receive what information and when it should be disclosed.

**Issue Resolution**

The resolution of a complaint may only affect a narrow segment of the company, as in the case of the correction of a single invoice or an expense report. Alternatively, a corrective action, for example terminating a senior executive for cheating or the restatement of previously issued financial statements, could be pervasive and far-reaching. In either case, preparing and adopting a formal corrective action plan is helpful. A corrective action plan sets out the matters to be addressed, the measurements to be used to determine success, the procedures to be performed, and actions to be taken to resolve a complaint.

The investigation team, management, the board of directors, or outside advisors may prepare the corrective action plan. In most cases, combined efforts of all these groups, along with input solicited from the outside auditors, legal counsel, and potential regulators, contribute to the plan. The highest level of oversight at the gaming company, usually the board of directors, should approve and adopt the plan. Before finalizing a corrective action plan, the directors will normally consult with management and external advisors to adequately consider company resource requirements and costs and to address practical limitations.

The corrective action plan should be monitored after implementation to ensure each matter is completed and satisfactorily addressed. Any material changes to the plan should be reported, reviewed, and approved by the board of directors. In some cases, the plan will call for action to be taken before an investigation is complete. For example, weak or compromised internal controls require immediate attention and remediation. Such actions should be documented and reported.
Reporting

Every action relating to an investigation will create curiosity. Interested parties may carefully monitor each step. Suspects may want their innocence to be communicated quickly. Guilty parties must be dealt with promptly and appropriately. The gaming company’s responsiveness shows that it takes complaints seriously and is prepared to deal with them. Therefore, thoughtful communication and reporting protocols are critical.

Investigation communication protocols must honor privacy, confidentiality and, as appropriate, anonymity. They also should provide a reasonable level of information to interested parties both inside and outside the company. Management, directors, investors, and employees require different treatment than regulators, auditors, creditors and the press. Gaming regulators may require that detailed reports of the investigations be maintained and subject to review and audit. Whistleblowers may expect reports on the status of their claims. Therefore, the preparation of good communication protocol may require the assistance of legal counsel, public relations professionals, and others to avoid liability for improper or incomplete disclosures.

In addition, to protect privacy, anonymity, and confidentiality, any materials collected as part of the investigation must be strictly controlled and secured. A well-documented chain of custody should be prepared and maintained, and the distribution and use of documents and reports restricted. However, the company should have a system in place to capture experiences related to handling complaints in order to avoid future problems or to identify best practices.

Retention

Materials, data, and reports produced during an investigation are evidence to be preserved, and retained according to company document retention policies and gaming laws and regulations. Once again, to protect sensitive information and the identities of certain parties to the investigation, care must be taken to limit access to hard copy documents and to store and secure electronic data and information. This material also serves as a record of the gaming company’s compliance with internal policies and procedures and federal and state control requirements.
The Overall Plan

Gaming companies should have processes in place to gather and investigate whistleblower complaints. The processes must ensure that all complaints are documented, investigated, and addressed in a timely and appropriate manner considering the interests of key stakeholders. The company must take a close look at its organization and determine the types of complaints likely to surface and prepare for crisis by establishing relationships with a range of experts available to assist should an investigation be required. It should train management and employees to use the process. Finally, gaming companies must create an environment of trust among those who may use the system, ensuring confidentiality and anonymity, as necessary. Ultimately, by doing this, the company can demonstrate compliance with regulatory expectations and organizational objectives to protect its valuable gaming license.
Chapter 7
RISK APPETITE: DETERMINING YOUR DIET PLAN

A gaming company’s regulatory compliance program is a key component of how the company manages risk attendant to criminal and regulatory violations by its officers, directors, and employees. Before designing the compliance program, companies often make the mistake of not first determining the risks and their likelihood and potential impact so as to design the most effective compliance program.

Gaming enterprises are subject to a number of risks ranging from criminal activity and civil regulatory violations to undesirable conduct. The management team for each gaming company must determine the types of risks present and how much of this risk is acceptable. After that, management should regularly assess the likelihood and potential impact in an effort to prioritize each type of risk. Risk exposure should be evaluated using quantitative and qualitative measures. Through gaming risk assessment, management can prepare and continually maintain a well-designed and effective compliance system to reduce risks to acceptable levels.

How Much Risk is Healthy to Swallow?

The Committee of Sponsoring Organizations of the Treadway Commission (“COSO”) defines corporate risk appetite and tolerance in its publication Enterprise Risk Management—Integrated Framework (www.coso.org). COSO states, “Both risk appetite and risk tolerance set boundaries of how much risk an entity is prepared to accept. Risk appetite is a higher level statement that considers broadly the levels of risks that management deems acceptable, while risk tolerances are narrower and set the acceptable level of variation around objectives.”

By way of analogy, risk appetite and tolerance are comparable to a diet. Risk appetite is the total number of calories a person can intake in a day to achieve a healthy diet, for example 2,500 calories. Risk tolerance is the number of calories that make up each meal in the diet. For instance, breakfast is limited to 600 calories, lunch 900 and dinner 1,000. Staying
Getting in the Game: A Guide to Successful Gaming Compliance

within risk tolerance levels (e.g., eating only the allowed number of calories for each meal) allows management to achieve desired results (e.g., achieve a healthy diet). COSO puts it this way, “Operating within risk tolerances provides management greater assurance that the company remains within its risk appetite, which, in turn, provides a higher degree of comfort that the company will achieve its objectives.”

Much like the recommended calorie intake to achieve a healthy diet will differ for individuals, so will risk appetites of each company. Some gaming management teams are risk adverse, while others see risk as an opportunity to increase financial returns. COSO frames the issue this way, “The level of risk that an entity is willing to accept is a management decision—and there is no right answer to this question. One company’s management will pursue a higher-risk strategy while another will pursue a lower-risk strategy.”

**Evaluation of Risks**

Two common methods are used to evaluate risks—quantitative and qualitative. Each method analyzes available information to help management determine the *likelihood* and *significance* of a risk. Determining the *likelihood* of risk requires probability predictions to assess the likelihood that an identified risk will actually be present in the workplace. *Significance* is usually measured in financial terms, and relates to risk magnitude and pervasiveness.

Quantitative methods rely on the analysis of data, usually large volumes of it, using proven models built on assumptions. Proven models are sound, generally accepted scientific, statistical or mathematical principles. The results are replicable using identical data and assumptions. However, as the “garbage in – garbage out” adage goes, quantitative methods depend heavily on accurate data, in sufficient amounts, obtained from reliable sources. Equally important are the assumptions used. Inaccurate, unreasonable or unsupported assumptions will yield unreliable results for risk assessment.

Qualitative methods are more judgmental and subjective than quantitative methods. Qualitative methods are frequently used in combination with quantitative methods. Alternatively, they may be employed when quantitative measures are inconclusive, when data is unreliable, or when the costs to
perform quantitative testing are prohibitive. Qualitative methods may include interviews, focus groups, surveys, and questionnaires. The results from qualitative methods are opinions about risk based on experience, knowledge, education, training and skills.

**Assessment of Risks**

An assessment of the likelihood and significance of risks caused by unacceptable or illegal conduct should be performed regularly. Frequency depends on a company’s business cycle, objectives and strategies. Obtaining feedback from management and key personnel is fundamental for an accurate assessment. Once gathered, information is then analyzed using qualitative and quantitative methods to estimate exposure to the business.

Knowledgeable personnel are a good starting point to identify risks. Gaming companies should engage management and employees in the risk identification process by interviewing, surveying or paneling focus groups. Management should be sure to involve executives in business units—such as accounting, human resources, and internal audit. This has the dual benefit of uncovering potential conduct risks and training personnel to be aware of such risks as part of their jobs.

Management also should consider past company experiences, industry information, business trends and plans, as well as international and cultural norms when identifying behavioral and conduct risks. Many gaming enterprises maintain a repository of lessons learned from prior violations and investigations. This corporate history is a great place to find risks requiring continued attention. Keeping abreast of the gaming industry and business trends is important, as changes in the form of legislation, labor shortages or technology could create some new risks and eliminate others. Of course, gaming companies should consider their own business plans, too. Plans for future expansion, the launch of information systems, or changes in senior management, just to name a few, can all impact risk. Finally, management must be mindful of any international operations and the unique risks that may arise from political, legal, and cultural behavior differences as compared to the United States.
Once identified, the likelihood of a conduct risk is measured by determining the expectancy of a criminal, unethical or noncompliant act happening in the workplace. The trick is not simply to list every possible risk, but instead to identify only those risks that are the most probable. That requires management to look at risk from two viewpoints—inherent risk and residual risk.

Risk is inherent with most bad acts because virtually everyone is capable of performing them under the right circumstances. In other words, even a good employee may violate behavioral standards when confronted with both pressure and opportunity. Residual risk, however, requires consideration of company controls that are intended to prevent or deter inherent risks from occurring. When evaluating residual risk, management needs to ask if its controls are appropriate and sufficient to reduce inherent risks to acceptable levels.

For risk events that are determined to be likely, management must estimate the significance of the risk to the company using both qualitative and quantitative methods noted. In some cases, this may be as simple as calculating the monetary impact of a single improper invoice or expense report on the company’s financial statements. For others, it may require a subjective prediction about possible adverse consequences and costs to the enterprise if, for example, a senior official violates gaming laws. In any event, management should estimate the significance of the impact of each risk, usually in monetary terms.

Total exposure measures the combination of likely and significant conduct risk exposure to the gaming company. Exposure is created when risks expected to have a significant adverse impact on the organization are likely to occur. Of course, exposure is affected if risks are interdependent or correlated. Corporate risk exposure should be quantified by management. This is accomplished by multiplying a probability percentage assigned to risk likelihood by the monetary significance of the risk. In other words, exposure is the result of how likely it is that a risk will occur in the workplace and its financial impact to the company.
The assessment of the likelihood, significance, and exposure of conduct risk to each gaming company should be performed periodically to coincide with short- and long-term business cycles, objectives, and strategies. The ebbs and flows of economic activity create business cycles. Typical cycles include seasonal retail sales patterns or peaks in gaming visits during holidays, summer breaks or around the time of notable sports events. From a short-term perspective, each spike in activity is a cycle related to a strategy that should be assessed. In the longer-term, risk assessments could be linked to three- to five-year business plans or overall business objectives. At a minimum, management should perform such an assessment at least annually to coincide with budgeting and financial statement preparation activities.

**Prioritization of Risks**

After exposure to criminal, unethical, inappropriate or noncompliant conduct risks is established, they should be prioritized by management. Some risks will be classified as top priorities; however, it is important that only truly critical risks receive this rating to prevent overloading management with too many matters at one time. During this process, it will become apparent that some risks, regardless of priority, require immediate action. Others will be handled over time with action strategically taken only after a study of costs versus benefits.

Successfully addressing high exposure risks will no doubt require investments, resources, organizational changes, strengthening of controls, and/or personnel changes. Risks classified as high priority should be addressed and monitored to ensure they are appropriately managed to acceptable levels. However, no risk should be ignored indefinitely. All other risks should be periodically reconsidered or reprioritized.
Gaming companies today are required to comply with multiple laws and regulations. They include the Sarbanes Oxley Act, Anti-Money Laundering Act/Bank Secrecy Act, Foreign Corrupt Practices Act, Payment Card Industry (PCI) regulations, and a number of minimum internal control standards and operating regulations issued by state agencies and the National Indian Gaming Commission, to name just a few. Although an internal audit function is an essential, if not required, part of monitoring and assessing compliance with laws and regulations, the purpose of internal audit is much broader. An internal audit helps management achieve its objectives and is defined by the Institute of Internal Auditors (“IIA”) as:

…an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

More than just verifying compliance, an internal audit can objectively assess whether the policies and procedures are adequate and effectively working to safeguard assets and control activities. While internal audits do not formulate policies and procedures, they make recommendations for improvement and can be called upon during the implementation and assessment of new processes and systems. Other duties of internal audits include the investigations of allegations related to fraud, waste, and abuse.

For management to maximize the full benefits, internal audits should become a partner with management and directors, helping to make the company successful through operational reviews that look for best practices to make processes run smoothly and efficiently. Unlike an external auditor, the internal auditor is around throughout the year and typically delves into more process detail. For example, for payroll or accounts payable activities,
an internal audit is tasked to find out not only if transactions are processed and controlled correctly, but also if the data is secure, efficiencies are in place to save costs, and proper segregation of duties exists, and to perform many other valuable duties.

Before internal audits can contribute to the success of the company, management and directors must ensure a sound foundation for operation and accountability. Some of the items to consider are as follows:

- **Professional Standards**—Knowledge and adherence to professional standards is critical for quality. The professional organization that governs how internal audit departments should be run is the Institute of Internal Auditors (IIA) (www.theiia.org). The purpose of the IIA’s Standards of the International Professional Practices Framework is to:
  - State basic principles for the practice of internal auditing;
  - Provide a framework for performing and promoting value-added internal audit activities;
  - Establish a basis for evaluating internal auditing performance; and
  - Improve organizational processes and performance.

- **Charter**—Any successful internal audit department needs a mandate to exist. The best mandate comes from an audit committee and is usually in the form of an internal audit charter. The charter gives the department its mission, authority, and even sets up its independence.

- **Staffing**—One of the key items is the people. An internal audit department needs individuals that have a good understanding of not only the organization, the industry, finances and operations, but countless other areas within a company. What may be more important than the staff is the leader, who recruits the auditors, sets the tone for the department and is an advocate for the team.

- **Support**—Senior management support of any undertaking within an organization is vital and an internal audit is no different. Without this, the company departments and other individuals will never respect or consider the internal audit group worthwhile. Behind any successful
internal audit department is senior leadership that supports them throughout the organization.

- **Quality**—A successful internal audit team has a demonstrated commitment to quality. *The IIA’s Quality Assessment Manual, 5th Edition*, breaks out the need for organizations to conduct both internal and external quality assessments to build and keep a strong internal audit activity working within the organization. The basic external quality assessment is a review of an internal audit department, where compliance is reviewed with regard to IIA standards, best practices and how well audits are conducted within an organization. Every internal audit department should have internal assessments or a full external assessment periodically. Many organizations, to include the IIA, are now requiring these assessments to report on the quality of work within an internal audit.

Once a company has set up the basics of its internal audit function, success is squarely in the hands of the personnel. To properly staff an internal audit, you not only have to fully understand the operating foundation, you also need to have well trained and experienced personnel in place to execute it. In general, an internal audit can be staffed in the following ways:

- **Internal**—This is an internal audit department staffed by employees who are fully integrated within a company. This department should be governed by IIA best practices and the lead internal auditor (also known as the Director of Internal Audit or Vice President of Audit) should report directly to the audit committee, with possible administrative reporting lines to either the chief executive officer or the chief financial officer. This arrangement preserves the independent nature of the internal audit department.

The benefits of an internally staffed internal audit department are that the internal auditors integrate into the company operations to understand the industry, business and personnel. In addition, the internally staffed internal audit department will have allegiance to the company and not a third-party provider.
The challenge is that companies must have enough internal audit staff to provide the critical mass to do the required amount of work, and they must constantly invest in training and technology. In addition, specialty skills may be needed for information technology, fraud examinations, financial reporting, gaming compliance, and many other areas.

• **Outsourced**—In this type of internal audit department, a third party provider is hired to provide internal audit services. A fully outsourced department comes in many flavors, but in general, the third-party provider performs risk assessments, planning, auditing, reporting, and briefs the Audit Committee with the findings.

The benefits of an outsourced internal audit function are that a company can bring in skilled providers on demand. This may also provide access to some of the best available talent in a particular industry with funding on a budget. In addition, these groups are truly independent, and are less likely to be affected by internal political and hierarchical pressures. Whistleblowers also may find outside providers more credible and objective when complaints are filed and investigated.

The primary disadvantage of outsourcing is that the auditors may not know your company or your industry as well as an internal employee. It may take longer to get necessary information and to complete assignments due to inefficiencies.

• **Co-sourced**—This internal audit function is a hybrid of the other two. A co-sourced department usually has some type of internal audit department in place within a company, but that department may not have the requisite skills necessary. According to the IIA’s *Establishing an Internal Auditing Activity Manual*, one of the most common co-sourced relationships is IT auditors. The benefits of this type of operation is the company partners with the co-sourced resources who can bring new perspectives and skills to an audit that may not be resident within the in-house department, while still getting the benefit of in-house employee knowledge.
With the ever-increasing requirements needed to run a successful gaming operation today, organizations must run efficiently, while still being compliant. One of the best ways to ensure compliance is through internal audit departments. An internal audit, when properly designed and staffed, can bring the ability and verify compliance with laws and regulations, while also partnering with management to ensure that operations run efficiently. In the future, experts believe that internal audit departments will continue to support more and more organizations, not only because of regulatory requirements, but because it makes good business sense.
Chapter 9
THE REGULATORY COMPLIANCE AUDIT
Glenn Light, Karl Rutledge and Quinton Singleton. Lewis & Roca LLP

Nevada’s gaming industry is in large part self-regulating. Gaming companies must take on the onerous task of drafting and submitting their compliance plans for approval to the Corporate Securities Division of the Nevada Gaming Control Board (“the Division”). Once approved and implemented, the Division regularly audits these compliance plans to ensure that companies are complying with their plans and to determine whether their company cultures embrace compliance. This chapter describes the overall audit process.

Selection for a compliance audit occurs on a periodic rotation. The Division maintains a master chart that details when the last audit was held for each gaming company and when the next audit is due. This methodology results in companies undergoing an audit approximately every two years. Selection also may occur, however, based on the conduct of a company. For example, if a company commits an egregious compliance violation, the Division will direct their attention to that company’s compliance plan and its adherence to it.

Depending upon the size of the company, the Division will typically assign one or two agents to conduct the audit, and it will take between one and two weeks to complete. A company can expect the agents to be physically present at the corporate headquarters throughout this period. The review will consider several regulatory objectives, such as:

• Are the compliance controls working?
• Do the compliance controls adequately detect the types of regulatory violations and crimes to which the company is vulnerable?
• Has the compliance program been modified or adapted to take into account any known criminal or regulatory violations?
• Should the compliance program be reviewed or updated to reflect any new company or industry threats or to reflect best practices within the industry?
For the company, the audit begins with the receipt of a document request letter from the Division detailing an initial list of documents the agents want to review. Typically, the Division will request access to the compliance plan and procedures, compliance committee minutes and due diligence checks. Following the request, an initial meeting will be held between the company’s compliance staff and the agents handling the audit. During this meeting, the compliance staff has the opportunity to express any thoughts or concerns regarding the company’s compliance plan. Likewise, the agents explain procedures and demystify the process. At this time, the compliance staff should provide the documents pursuant to the Division’s earlier request. This is only the first production of documentation, as additional requests are likely throughout the audit. These requests can be broad and be directed at documents in any area of the gaming company’s operations. Compliance plans customarily have policies that all personnel must respond to requests by the gaming authorities for access to books, documents, records, and papers relating to the company’s business activities. Willful failure to comply with the directive is usually grounds for summary termination of employment.

After the initial conference, the agents review the company’s compliance plan. The agents begin by preparing a matrix of the company’s compliance plan to crosscheck the files to ensure the company is conducting appropriate safeguards and vetting. Generally, each plan has mandated activities requiring due diligence reviews of those vendors, suppliers, lobbyists, key employees, and consultants whose compensation or other payments are material because they exceed designated financial thresholds. A crucial ingredient of the audit, therefore, becomes whether the activities that trigger these requirements are being recognized and that the company conducted the appropriate due diligence once triggered.

The Division does not, however, want these audits to become full blown investigations. Agents typically only thoroughly examine a sample of the files to ensure the company is faithfully following their approved plan. They analyze and verify transactions, and review organizational and functional activities. For instance, the company may have had the obligation to conduct due diligence on 120 vendors transactions for the period in which
the agents are investigating. The agents may discover, however, that the company failed to address 12 of those transactions. Consequently, the agents note these omissions and address them both in their report and in a conference with the compliance staff to make sure the company remedies these omissions in the future.

The audit also evaluates the compliance committee minutes to assess the adequacy and effectiveness of compliance controls and to determine if the committee is following the company’s instituted policies and procedures. In particular, the agents look to see if the committee is being notified of the issues and whether, when notified, is diligently and knowledgeably discussing the presented issues. As important as recognizing what activities trigger due diligence requirements is the commitment of the company to actively engage in meaningful discussions of those activities.

Once the agents complete the on-site audit, they compile a report of their findings. The report lists the areas analyzed in the audit, notes the areas where the company was proficient, but most importantly, analyzes areas of deficiency. The most common shortcoming involves companies not undertaking proper and complete due diligence of individuals, vendors and suppliers as required by their compliance plans.

Other common violations found in compliance audits include:

- Failure to keep adequate records, e.g., records do not go far enough back, cannot be located, or do not exist.
- Failure of segregated company divisions to understand when compliance actions should be taken and then failure to forward compliance issues to the compliance officer or compliance committee.

For example, a sales representative for a manufacturer/distributor conducts a sale of gaming equipment that exceeds a particular monetary threshold and as such should be reported to the compliance officer; however, the sale is not reported, either because of a failure of the segregated divisions to inform each other of the requirements or an internal failure on behalf of the company to demonstrate to the divisions the importance of such compliance.
• Failure to provide the compliance committee with all relevant information necessary to properly perform compliance duties.

While these shortfalls are not minor, the compliance staff typically can remedy many of them simply through awareness and education. For that reason, the Division strives to complete the write-up process within a month. Due to excessive workloads and the possibility of being called off the audit to work on licensing projects, the audit report can be delayed, however, sometimes by as much as a year.

After the report is compiled, the agent(s) meet with either the Chief or Deputy Chief of the Corporate Securities Division. The report is then forwarded to all three members of the Gaming Control Board for their review and on occasion, the Gaming Commission. From this point on, the company will hear little unless the report uncovers serious compliance violations and the Board or Commission decides to pursue disciplinary actions.

The close of the compliance audit occurs with the Chief or Deputy Chief’s meeting with the company’s compliance staff to explain their findings. At this time, company officials can ask questions or recommend changes they feel would be beneficial to the company and the compliance plan. Often the Division and the board are amendable to modifying the existing plans as requested by companies to improve efficiency of the compliance process. The board’s focus is on not only effective but also practical plans that the company will embrace to ensure the culture of corporate compliance within Nevada gaming companies.

In the past, company personnel often viewed compliance plans and officers as unwanted and incommodious interferences with business operations. This perception, however, is changing. Through the use of these audits, the Nevada Gaming Authorities endeavor to make compliance a prolific and central focus of gaming companies to ensure that they not only comply with the letter of the law but also establish compliance as an integral part of their company culture.
Chapter 10
SECURITIES ISSUES: INSIDER TRADING AND FALSE OR MISLEADING DISCLOSURE

For U.S.-based public gaming enterprises, the threat of an illegal insider trading scandal may jeopardize a gaming license, or even the survival of the business itself. The alleged use of non-public information for unwarranted personal gain quickly destroys the trust of shareholders and regulators in the company and its executive team. To address this risk, companies employ policies and procedures, signed executive compliance statements and oversight by compliance officers, among other things. However, many do not adequately bridge the gap between these techniques and the practices, policies, and procedures governing gaming activities.

Many publicly held gaming companies have failed to include provisions for insider trading in their gaming compliance policies and procedures, and likewise have ignored the need to train officers, directors, and employees on this serious matter. Interlacing existing insider trading policies and procedures with the gaming compliance program, and then instructing personnel on how to understand and use the materials, provides an extra safeguard to ensure compliance. Taking advantage of the expertise of the gaming compliance officer when developing training programs and implementing the plan across all facets of the business is also advisable. These types of activities help to maintain the integrity and reputation of the company, especially with gaming regulators.

Insider Trading Defined

Insider trading has many definitions and connotations that encompass both legal and prohibited activities. The legal version of insider trading occurs when company insiders—officers, directors or employees—buy or sell stock or other securities in their own companies within the confines of company policy and the governing security regulations. The public can track insider trades by virtue of publicly filed reports required by securities regulations. The illegal version of insider trading, on the other hand, refers to the prohibited practice under federal and state statutes of buying or selling a public company’s stock or securities in breach of a fiduciary duty or
other relationship of trust and confidence while in possession of material, non-public information. This type of insider trading achieved wide-spread notoriety in the 1980s with a large number of indictments of notable executive by the Securities and Exchange Commission and the United States Department of Justice. It seems this also inspired Hollywood’s imagination, with the production and release of the movie “Wall Street”.

The theory behind the prohibition on insider trading is that it undermines investor confidence in the fairness and integrity of the securities markets. Trades made by insiders, based on “material” non-public information, are considered to be fraudulent because the insiders are violating the trust or the fiduciary duty that they owe to the shareholders and the public at large. A major Federal Appellate Court decision (List v. Fashion Park Inc., 340 F.2d 457, 462 (1965)) noted that “the basic test for materiality ... is whether a reasonable man would attach importance ... in determining his choice of action in the transaction in question.” In other words, if an investor would likely consider the information important regarding the purchase or sale of stock and securities, then it is deemed material.

**Federal Regulation**

Following the United States stock market crash of 1929, Congress enacted the Securities Act of 1933 and Securities Exchange Act of 1934 (“SEA of 1934”), in part, to keep the public securities markets free from fraud and to control the abuses believed to have contributed to the crash. Two specific statutes govern insider trading: Section 16(b) and Section 10(b) of the SEA of 1934.

In summary, Section 16(b) of the SEA of 1934 prohibits short-swing profits by corporate insiders in their own company’s stock. According to Section 16(b) “corporate insiders” are the company officers (e.g., president, vice president, chief financial officer, etc.), directors and any other beneficial owners of more than ten percent (10%) of the company’s equity securities. Section 16(b) is applied mechanically, and generally requires that any prohibited profits realized on a buy and sell (or sell and buy) of a security within a six-month period by an officer, director or 10% shareholder are recoverable by the corporation. Any buy and/or sell transaction of
securities within a six-month period is typically actionable, and there is no requirement to show that the insider actually traded while possessing material, non-public information. Any shareholder can bring an action under this section of the SEA of 1934.

“Insiders,” however, can go beyond officers, directors and 10% shareholders. Section 10(b) of the SEA of 1934, as implemented by Rule 10b-5 of the Security Exchange Commission (“SEC”), makes it unlawful for an individual to engage in fraud or misrepresentation in connection with the purchase or sale of a security. Under these provisions, the Courts have expanded the scope of insider trading by, in part, considering trades by certain “corporate insiders” to be fraudulent. This would apply to individuals whose “relationship of trust” is much more remote in nature than that of a fiduciary like an officer or director.

For example, in 1997 the Supreme Court embraced a “misappropriation” theory of omissions, holding that misappropriating confidential information for securities trading purposes, in breach of a duty owed to the source of that information, gives rise to a duty to either disclose that information or abstain from trading activities. Although the law on insider trading in the United States is continuing to evolve, existing law basically requires that any insider having material information with regards to a corporation is prohibited from trading, based on that knowledge, until the information is available to the general public. Rule 10b5-2 now clarifies how the misappropriation theory applies to certain non-business relationships by stating, among other things, that a person receiving confidential information would generally owe a duty of trust or confidence and may be liable under the misappropriation theory. Simply put, these persons must either disclose that information or abstain from trading public securities.

**Violations of Insider Trading**

This situation has encouraged governmental regulators, enforcement agencies and several stock exchanges to actively monitor, investigate and prosecute illegal securities trading activities among a wide group of investors. These entities search for suspicious or unusual trades and trading activity levels. Unexplained transactions trigger inquiries and, potentially,
full blown investigations. Allegations of illegal insider trading may result in enforcement action by federal and state agencies. For example, the SEA of 1934 permits the federal government to bring suit against insiders alleged to have engaged in illegal securities trades to seek injunctions, recover any illegal gains (or losses avoided), and/or impose civil penalties, the amount of which may be up to three times the profit gained (or loss avoided). In addition, public trading can be halted on the company’s securities. U.S. governmental agencies prosecute over 50 such cases each year.

The effect of broadened powers has also led to U.S. and state governmental agents prosecuting a variety of persons for insider trading beyond corporate officers, directors, employees and significant shareholders. Indicted individuals have included friends, business associates and family members of insiders. Prosecution has also implicated other “tippees,” such as attorneys, bankers, brokers, employees of printing firms and government employees. In most cases, these parties obtained material, non-public information by virtue of their relationships with the company or persons within the company.

**Gaming Company Solutions**

Gaming companies can leverage their gaming compliance plans to avoid insider trading problems in significant ways. Reinforcing policies designed to ensure the confidentiality of certain company information until its general release to the public using training, monitoring activities and effective whistleblower programs is one way. All gaming enterprise officers, directors and employees should be educated about insider trading policies and procedures, linked specifically to gaming compliance activities, and encouraged to confirm this understanding annually in writing. They should also be taught how to recognize suspicious activity and how to report these events promptly to appropriate supervisory-level personnel or by using whistleblower systems. Key vendors and other parties should also receive communication about the policy requirements, together with instructions to report suspected violations. Efforts like these will help manage material financial information, both positive and negative, so that it is appropriately safeguarded until released by officers and directors, and then released consistently and disseminated broadly to the public at large.
Another way to avoid insider trading problems is to recognize that not all potentially illegal insider information is in the form of material financial information, but may include plans, expectations and negotiations. Consider the possible importance of information such as the imminent issuance of a gaming license, the results of a pending bid to build a casino, labor disputes, joint ventures or mergers with third parties, impending financial problems, results of trials or significant litigation exposure due to actual or threatened litigation, changes in senior management or the announcement of new construction projects. As you can tell from this listing, the possibilities are limitless. To address this matter, gaming companies must train all insiders about potential improper disclosures and trading activities, and the protocols to report and handle them.

Well crafted guidelines also can help gaming enterprises prevent incidences that could result in civil or criminal actions, shareholder suits or regulatory issues related to allegations of insider trading. Guidelines presented in simple, understandable language about the day-to-day usage of compliance policies are easy to use and apply. Such guidelines might prohibit activities like sharing confidential and proprietary non-public information or encourage personnel to refrain from commenting on analyst projections or any releases of forward-looking information. Requiring employees to obtain approvals before making any public presentations of company information, a common occurrence at any of the many gaming trade shows or conferences, may also be important.

Formally, a publicly-traded gaming company’s directives may specifically prohibit officers, directors or certain employees from conducting any trades for a set period of time after the company has made a public announcement of material information, including earnings releases. It should also give guidance or “windows” as to when trades are permitted and it must require that any officer, director or employee possessing material non-public information is prohibited from trading on that information even during an open “window” period, unless required disclosures have been appropriately made. In addition, it is recommended that policies govern certain types of trades such as puts, calls, and short sales.
A simple method for bringing insider trading activity to the attention of management and directors is to have personnel report all securities transactions to the compliance officer or another designated official. In particular, major securities holders, officers and directors may be required to report holdings and activity to the compliance officer. In this way, relevant transactions are noticed and can be tracked and periodically reported to other company officials and governmental agencies, as necessary. Transactions can also be subjected to pre-clearance procedures to protect the company. In problematic situations, personnel can be encouraged to report suspicious activity related to insiders to the compliance officer. However, as mentioned above, whistleblower programs also may be an effective way to learn about these events.

**Linking Insider Trading Directives with Gaming Compliance**

Public gaming companies face significant business risks from the failure to recognize and report insider trading activity. In the past, federal and state regulators have aggressively prosecuted suspected violations of insider trading rules, placing company officials and the enterprise in the direct line of harm. To address this issue, gaming companies should consider linking insider trading directives with gaming compliance policies and procedures. Once integrated, insiders, including officers, directors, major shareholders and employees, can be trained to recognize and report suspected improper trading activities to appropriate company officials. Everyone considered the recipient of insider information can then work effectively together to manage the risk of illegal trading and its effect on gaming compliance.
Chapter 11
THE BANK SecRECY ACT AND ANTI-MONEy LAUNdERING
Meredith Jonas and Kelly Gentenaar, Grant Thornton LLP

The Bank Secrecy Act (BSA) was enacted by Congress in 1970 in response to increasing reports of people bringing bags full of currency of doubtful origin into banks for deposit. The implementation of BSA regulations, specifically 31 CFR 103 (commonly referred to as “Title 31”) of the act, resulted in financial institutions being required to file reports with the federal government regarding the activities of their customers. These reporting requirements were intended to prevent banks and other financial service providers from being used as intermediaries for criminal activity.

Casinos, which offer a broad array of financial services, including customer deposits or credit accounts, facilities for transmitting and receiving funds directly from other institutions, check cashing, and currency exchange services similar to services of depository institutions, must comply with BSA regulations.

Originally regarded as merely recordkeeping rules for financial institutions, BSA reporting requirements have become more robust amid changes in the U.S. financial system. As a result, BSA information reported by financial institutions has become an essential source of information for law enforcement and federal agencies to conduct investigations of criminal activities within and safeguard the integrity of the U.S. financial system. In this context, financial institutions—the definition of which includes gaming companies—that are subject to the BSA reporting requirements provide critical information in conducting their regulatory compliance efforts. A lack of BSA regulatory compliance can not only result in fines and punitive actions from regulators, but can also result in entities becoming the unwitting accomplices in criminal activities.

In the nearly 40-year period since its passage, Congress has enacted numerous amendments to the BSA. These amendments were not only intended to enhance law enforcement effectiveness, but also to keep pace with the rapidly globalizing financial systems and the criminal activities
within these systems. The most notable of these amendments was the USA PATRIOT Act of 2001 (Patriot Act), an amendment passed as a consequence of September 11th. The Patriot Act has played a crucial role in increasing the awareness of money laundering and the financing of terrorism by requiring financial institutions to increase the amount of information gathered under the BSA and implement an anti-money laundering (AML) program.

As complexities grow in the global financial markets, the U.S. financial system’s vulnerability to financial crimes also increases. AML programs have become one of the U.S. financial system’s first lines of defense against these vulnerabilities.

Financial institutions armed with sound BSA compliance programs that require increased due diligence and reporting are better equipped to:

- Ensure regulatory compliance in an increasingly complex global financial system.
- Combat the threat of money laundering throughout the financial system.
- Detect, prevent and respond to criminal activities.

Further, AML programs give financial institutions an increased ability to identify criminals at one of the most vulnerable points in the money laundering cycle: when funds are introduced into the financial network.

The U.S. Department of the Treasury designated the Financial Crimes Enforcement Network (FinCEN) as the administrator of the BSA in 1994. In this role, FinCEN promulgates regulations, provides outreach and guidance to the regulated industries, and pursues civil enforcement actions in certain circumstances. In addition, FinCEN analyzes and reviews information reported through BSA requirements by financial institutions. BSA databases, including the Currency and Banking Retrieval System (CBRS) and Currency and Banking Query System (CBQS), exist for the use of law enforcement and regulatory agents. CBRS is the primary database for BSA records, including Currency Transaction Reports (CTRs), reports on foreign bank and financial reports, and Suspicious Activity Reports (SARs). CBRS, which is maintained by the Internal Revenue Service, Detroit Computing Center,
is used by regulatory and law enforcement staff. The CBQS, another repository of SAR information, allows law enforcement and regulators the ability to query fields within SARs.

**Casinos and AML Compliance Programs**

As fast-paced, cash-intensive businesses that provide a financial product in the form of gaming—including a broad array of financial services akin to that of depository institutions—casinos have long been identified as entities that are vulnerable to abuse by money launderers and tax evaders. The BSA regulatory environment specific to casinos addresses these inherent vulnerabilities and has undergone a great deal of change to keep up with the changing gaming landscape since state licensed gambling casinos were generally made subject to the BSA as of May 7, 1985. However, the overarching objective of the BSA—to prevent financial service providers from being used as intermediaries for criminal activity—has not changed. Casino operators should be mindful of this objective as they implement their AML compliance programs and subsequent reporting requirements.

Casinos are included in the BSA definition of “financial institution” as any “casino, gambling casino, or gaming establishment with an annual gaming revenue of more than $1,000,000 which is licensed as a casino, gambling casino, or gaming establishment under the laws of any state or any political subdivision of any state; or is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation which is limited to class I gaming (as defined in section 4(6) of such Act).” (31 U.S.C. section 5312(a)(2))

A casino’s AML compliance program should be developed using a risk-based approach to address products and services, customers, geographic areas, and transaction types. At a minimum, the AML compliance program must include:

- An independent internal testing function.
- Independent testing (internal or external) for compliance with the BSA regulations.
- A designated compliance officer to perform on-going monitoring.
- An AML training program.
Once the AML compliance program has been developed, a best practice for casino operators (although not required in section 103.64 of the regulation) is to obtain board of director, or other oversight body, approval of the written compliance program, and evidence this approval in the board’s meeting minutes. Following the approval of the AML compliance plan, a compliance officer should be designated to implement and oversee and monitor the program.

To increase the effectiveness of its AML program, the casino should implement training programs that educate employees on money laundering “red flags” and current regulatory reporting requirements specific to the gaming industry. A thoughtful, well-founded and well-documented AML program is most effective if the overall objectives of the plan and procedures for implementing are communicated to those directly affected by the regulations, including front line employees such as cashiers or dealers.

**Casino Reporting Requirements**

Casinos or card clubs (both land-based and riverboat operations) with gross annual gaming revenue in excess of $1 million are subject to the BSA casino regulatory requirements. To comply with BSA regulations, casinos must report certain currency payments as well as suspicious activity identified within the casino. The forms used to report such activities are FinCEN Form 103: Currency Transaction Reports by Casinos (CTRC) and FinCEN Form 102: (Suspicious Activity Report by Casinos and Card Clubs, SARC).

Casinos are required to file a CTRC for all cash transactions exceeding the $10,000 reporting threshold, either individually or in the aggregate, in one gaming day. However, FinCEN has amended BSA regulations on casino reporting requirements for certain currency transactions. Specifically, “reportable transactions in currency, jackpots from slot machines and video lottery terminals, as well as transactions, under certain conditions, involving certain money plays and bills inserted into electronic gaming devices” are exempt from BSA filing regulations (see 72 FR 35008 (June 26, 2007).

Besides the standard CTRCs filed for a single currency transaction, casinos are required to file CTRCs for reportable multiple transactions identified through the aggregation of daily records. The process of consolidating...
accounting records, daily gaming activity logs and other electronically stored information to determine aggregate daily totals must be performed to assist the casino in its efforts to comply with BSA regulations. If reportable multiple transactions are identified, the casino must attempt to identify the customer using all records available, including any electronic data or previously filed BSA forms and tax forms. As such, records used to assist with customer verification must be periodically updated to ensure their accuracy. While the casino must make every effort to identify customers for CTRCs, FinCEN does recognize that not all customers will be able to be identified due to the nature of gaming activities.

While all suspicious activity may not warrant a CTRC on the basis of the currency transaction value, a SARC must be filed if suspicious activity is identified within the casino. Casinos are required to file a SARC if they identify a suspicious activity, whether attempted or completed, which involves $5,000 or more in funds or other assets. Similar to the AML compliance program as a whole, internal controls to detect suspicious activity must be developed using a risk-based approach for the areas of products and services, customers, geographic areas, and transaction types.

In an effort to assist law enforcement agencies and other regulatory bodies with criminal and/or civil investigations involving BSA records, FinCEN recently reported that law enforcement agencies have found the following types of information particularly useful during the course of their investigations:

1. Complete subject identifying information, such as name, permanent address, government-issued identification number, date of birth and casino account number.
2. Characterization of suspicious activity by checking Item 26 on the form and only checking the “other” box if the activity is not covered by the existing list of suspicious activities.
3. A concise and clear narrative that provides a complete description of the suspicious activity. Concise and clear SARC narratives (i.e., Part VI) include the following:

Getting in the Game: A Guide to Successful Gaming Compliance

- provides a detailed description of the suspicious activity;
- does not state, “See attached”;
- identifies “who,” “what,” “when,” “why,” “where” and “how”;
- identifies whether the transaction was attempted or completed;
- is chronological and complete;
- identifies the dates of any previously filed Form 102 on the same subject;
- notes any actions (taken or planned) by the casino, including any internal investigative measures used by the casino to maintain records of the suspicious activity; and
- includes contact information for persons at the casino with additional information about the suspicious activity.

The recently launched FinCEN casino-specific Web site also provides the casino industry with BSA compliance information (available at http://www.fincen.gov/financial_institutions/casinos/).

**Application of BSA Information: The End Result**

FinCEN’s most recent publication, *SAR Activity Review: Tips and Issues* (May 2008), highlights the importance of BSA information obtained from casinos. As described in the article, a fraud offender was indicted by a federal grand jury and sentenced to imprisonment, supervised release, full financial disclosure, and restitution amounting to several hundred thousand dollars. Subsequently, it was determined that the convicted criminal was delinquent on restitution, and an investigation was ordered. BSA records uncovered CTRs from two casinos that amounted to more than $500,000 of unreported personal income. After review of these BSA records, casino gaming records were obtained to determine gambling activity to support violations of supervised release procedures. These findings resulted in additional charges, including restitution, supervised release, and full financial disclosure, being filed against the individual because such activity was in violation of his sentencing.
Chapter 12
CAMPAIGN CONTRIBUTIONS

Gaming companies, like all companies, are subject to a myriad of federal and state laws governing their involvement in political campaigns. The federal campaign laws are common to all corporations and restrict or prohibit both hard and soft money contributions to candidates for federal office or used to influence federal elections. Likewise, most states have campaign laws that may restrict or prohibit the involvement of corporations in state or local elections.

Unlike other corporations, however, gaming companies and their officers, employees, directors and some shareholders also may be subject to special state campaign laws that apply only to casinos. For example, New Jersey has a policy preventing certain casino personnel from contributing to state political campaigns or even from soliciting others to contribute to such campaigns. The purpose of the New Jersey ban is to isolate the industry and diminish its ability to influence the political process. Persons included within this prohibition are applicants for or holders of a casino license; any of their holding, intermediary or subsidiary companies; any officer, director, casino key employee or principal employee of any of these companies; or any person or agent acting for any of these companies or persons.

Violations of campaign laws can have serious ramifications for gaming companies. On the federal level, the Federal Election Commission (the “Commission”) has exclusive jurisdiction over the civil enforcement of the federal campaign finance law. Enforcement actions are initiated by Commission staff or by complaints filed by outside individuals or groups. If alleged violations are substantiated after investigation, a corporation could be subject to a significant fine.

Beyond fines, violation of campaign laws has had significant ramifications to gaming licensees and applicants for gaming licenses. In 2003, two suppliers in Michigan were denied applications because they made political contributions to Michigan candidates after filing their applications, in violation of Michigan state law. In 2000, a Las Vegas casino paid a $475,000 penalty for sending a mailer designed to discredit an elected official that was up for reelection,
in violation of state campaign laws. The company blamed the lapse on the failure to adequately supervise the employees due to the company’s rapid growth. Such a failure could have been avoided with proper supervision provided by a comprehensive compliance plan.

The rules and restrictions regarding political activity by gaming companies can be quite complex. They can govern diverse areas such as direct contributions to candidates, soft money spent for campaign purposes outside of contribution limits often for external “electioneering communications,” internal company communications regarding political elections, and the creation and funding of Political Action Committees.

The purpose of including political activity in the gaming company's compliance plan is not to assure corporate compliance with all campaign laws. Rather, the compliance plan is generally intended to assure that the company’s employees are not engaged in activities that could result in a campaign law violation. For example, whether the company should decide to set up and administer a Political Action Committee is within the purview of management; however, compliance can be verified through legal counsel outside of the compliance plan. Areas typically covered in a campaign compliance plan include prohibitions for gaming employees making campaign contributions, standards regarding political solicitations and other political activity, and restrictions on external and internal communications.

**Assuring Gaming Employees Do Not Violate Prohibitions**

The Federal Election Campaign Act of 1971 (the “Act”) was initially passed to increase disclosure of contributions for federal campaigns. The Act was amended in 1974 to limit campaign contributions. Specifically, for profit corporations were prohibited from contributing directly to federal candidates, national party committees, or even state party committees for federal accounts. These are often referred to as “hard money” contributions.

A well-designed campaign contributions compliance plan will identify any federal and state prohibitions or limitations and properly instruct all gaming personnel regarding their rights and obligations under the law. For example, the plan should clearly provide that no funds or assets of
the gaming company can be used for federal campaign contributions. The plan should further reflect any state (or foreign) restrictions on campaign contributions. This should extend to situations where the contribution is in payment for an event or item such as the purchase of tickets to special dinners that support a candidate or a political party.

Most importantly, the plan should be designed to create procedures to assure that gaming corporate personnel do not inadvertently violate hard money campaign prohibitions by providing in-kind contributions. Federal law defines a “contribution” to include “anything of value” given to a federal candidate or committee. This definition encompasses in-kind contributions such as office, meeting or convention space and equipment, transportation or fundraising expenses. In the context of a casino, in-kind donations could include providing banquet space, complimentary food, beverages or lodging, or free use of casino-owned transportation.

In situations where contributions are permitted in state or local elections, the campaign compliance plan should set procedures for approval of permitted contributions and a mechanism to ensure contributions are captured and reported. Gaming companies must avoid the appearance of a political monetary contribution looking like a bribe. To avoid these issues, the compliance plan should assure complete transparency. In other words, the company must document and record the amount or origin of each contribution and the recipient. The plan also can limit the nature of the contributions, for example, to prohibit cash contributions and to assure that they are made only to an authorized campaign committee or other appropriate party. Centralized reporting within the company can assure that the contributions are properly reported and do not exceed any contribution limits.

Standards Regarding Solicitations and Political Activity

The viability of representative government depends upon the political election process, and most companies encourage their employees, as individual citizens, to participate freely and actively in the political process and to make personal political contributions to candidates, parties and committees of their choice. The campaign compliance plan, however, should
make clear the distinction between private activity and actions taken as an employee. The plan may segregate these two roles by prohibiting political activity on company time and using company resources.

Under no circumstances, however, shall any employee be compensated or reimbursed in any way for any personal political contribution, or favored or prejudiced in any condition of employment or promotion by making or failing to make, any contribution. This could constitute a direct violation of prohibitions against hard money contributions and other campaign laws. The plan also can be drafted to avoid any question as to whether an employee is intimidated into or rewarded for contributing by prohibiting officers, directors or employees from soliciting contributions to any political candidate, campaign, party or ballot initiative from any other officer, director or employee, without regard to where such solicitation takes place.

**Restrictions on Communications**

A gaming corporation may spend funds on communications directed to its own members, known as internal communications. These consist of internally-focused communications to shareholders, executives and administrative personnel. These communications can be on any subject, including partisan endorsement in a particular campaign.

External communications, messages to parties outside the gaming corporation, however, may be subject to state and federal regulation or prohibition. For example, the Bipartisan Campaign Reform Act prohibits corporations from contributing “soft money” to both federal and state candidates and national, state, and local political parties for “electioneering communications.” This includes electioneering communications that through broadcast, cable, and satellite communications identify a candidate for federal office and are aired within 60 days before a general election or 30 days before a primary election, and can be received by 50,000 or more people in the jurisdiction the candidate seeks to represent.

Compliance plans should instruct employees as to the required procedures for approval of all internal or external communications prior to distribution. This simple requirement may have saved almost a half million dollars in fines to that Las Vegas casino mentioned earlier.
With increased U.S. Securities and Exchange Commission (SEC) and the Department of Justice (DOJ) scrutiny on U.S. companies’ business practices in foreign countries, a myopic focus on U.S. policies and procedures can detract from oversight of Foreign Corrupt Practices Act (FCPA) violations.

In the wake of the Sarbanes–Oxley Act of 2002, companies have invested significant time and money to ensure compliance with U.S. laws and regulations. However, these laws and regulations are the Achilles’ heel of many U.S. companies with foreign operations. In particular, significant risks exist when companies neglect to monitor for violations of the FCPA.

While the FCPA has been in place since the 1970s, there has been a recent spike in investigations by both the SEC and the DOJ. This current trend is the result of companies moving more aggressively into emerging markets like India and China, where anti-bribery laws tend to be somewhat lax.

Provisions of Sarbanes-Oxley itself are another reason why scrutiny of FCPA violations has increased. Not only is there overall concern with corporate governance, prompting regulators to increase their watchfulness, but an important Sarbanes-Oxley provision encourages companies to set up whistleblower programs to facilitate the reporting of fraud and other illegal activity. Whistleblower programs have been proven to increase the reporting of suspicious activity.

Furthermore, since FCPA violations such as bribes and money laundering are often associated with terrorism, the DOJ has stepped up its vigilance.

Penalties for violating the FCPA can be harsh. Companies that pay off foreign officials are liable for up to $2 million, or twice the gross gain or loss derived from the bribe. Individuals found guilty of paying off foreign officials
can be fined up to $250,000, or twice the gross gain or loss derived, and can incur a prison sentence of up to five years. Companies found guilty of improper and misleading recordkeeping can pay up to $2.5 million in fines. The repercussions for individuals guilty of improper and misleading recordkeeping are even more severe; these include a maximum $1 million fine and up to 10 years in prison.

**Pitfalls of Emerging Markets**

Many companies fail to evaluate the risks before entering a new market. Often, poorly trained employees assume a “when-in-Rome” attitude, not realizing that the local way of doing business may be a direct violation of U.S. laws and regulations. It does not help that U.S. companies that abide by these laws and regulations tend to face an uneven playing field, sometimes losing out to competitors from countries that do not adhere to such practices. Even when other countries do have similar legislation, it is not necessarily enforced with the same vigor as in the U.S.

Prior to beginning business in a new country, it is important to thoroughly research the business environment. The global organization, Transparency International (www.transparency.org), compiles a “corruption index” every year to help companies understand the potential risks arising in certain countries.

When trying to penetrate a new market, businesses will often hire agents or consultants to assist with activities such as obtaining licenses. These individuals know the local business community and have access to the right government officials; when they offer legitimate assistance, they are a real asset. However, agents can pose risks because while some act properly, others do not. Often, relatives of foreign officials who have decision-making authority may set up consulting firms to facilitate transactions for foreign businesses. Paying individuals in such positions of influence can be considered a violation of the FCPA.

Conducting a full background investigation of any agent or consultant they hire is critical for companies. Some federal agencies like the Department of Commerce and the Department of State will even assist with that process (they keep lists of individuals who have had previous FCPA violations). Such
due diligence has an additional benefit: it creates a document trail that may be important if, despite its best efforts, a company is subject to an investigation. The company will then be able to show that it acted in good faith and tried to detect and deter FCPA violations.

Nevertheless, a background investigation is not always enough. Even after agents receive the green light, companies must continually monitor agent and employee activity.

For example, if a company is paying an agent a flat fee for services and reimbursing expenses, the agent must show how that money is being used. Also, an agent’s contract should clearly state that any violation of the FCPA is unacceptable—because ultimately, the company can be held liable for that agent’s actions.

The FCPA does acknowledge the complexities of conducting business in emerging markets. It includes exceptions that allow certain payments to help ease the transition into a country. These payments must be aimed at facilitating government procedures, as opposed to sidestepping them. For example, a company can hire an agency to facilitate the processing of employee passports and other paperwork. Similarly, many companies hire local representatives to help move equipment through customs quickly. This is normally considered legitimate, as long as the agency is not linked to government officials who oversee the process. The FCPA also allows companies to hire police protection to keep their employees safe.

**Monitoring Behavior**

To identify violations before the SEC does, companies should be aware of the following red flags:

- **Payments going offshore or to unusual addresses.** People involved in illegal activity want to put money in places where their government cannot get at it. For example, in Russia, payments may be going to the Cayman Islands. The Office of Foreign Assets Control (www.ustreas.gov/ofac) and the Financial Crimes Enforcement Network (www.fincen.gov) both offer lists of known money laundering havens.
• **Frequent cash disbursements.** Distribution of large cash sums is often an indication that bribes are being doled out.

  – *Over-utilized accounts.* Accounts that cover payments for intangible services are often used to veil illegal payoffs. For example, if the legal accounts or consulting accounts appear over-utilized, it is possible that illegal payoffs are being made. Companies should pay particular attention to activity in these accounts and demand supporting documentation for services rendered.

  – *Lack of proper approval process.* Wire transfers typically require the sign-off of two high-ranking officials. However, employees involved in bribery or money laundering will often verbally approve wire transfers because they do not want their signature on such transactions. Companies need to look for instances where managers have opted to override these internal controls.

  – *Deals with complex legal structures.* When there are several layers of lawyers involved in a transaction, it is easy to lose track of payment flows. Funds that are ostensibly used to cover business meetings necessary for hashing out the details of a complex contract might instead be used for bribes. These types of expenditures should be examined closely, particularly when multiple firms are involved.

  – *Unusually high or low profit margins on projects.* Profit margins cannot always be taken at face value. For example, profit margins might be high because no work is being performed. Very often, this red flag is ignored; it must be considered whether foreign operations are losing or making too much money.

  – *Payments in round dollar amounts.* The Bank Secrecy Act requires financial institutions to report suspicious cash transactions. There is also a dollar threshold of $10,000, above which the filing of a Currency Transaction Report or a Suspicious Activity Report is required. Thus, companies involved in money-laundering will often transfer funds in amounts just below the $10,000 reporting threshold, but often still in round numbers. If a company observes a
series of transactions in round dollar amounts below the reporting threshold, this is a pattern that is consistent with money laundering activity and should be investigated.

**Education and Communication**

While it helps to know how to spot violations, knowing how to prevent them is even more important. The companies that are most successful in deterring FCPA violations usually do the following:

- **Educate employees about laws, regulations and internal policies.** Employees being sent to manage foreign operations need to fully understand the provisions of the FCPA. Best-practice companies develop detailed training with interactive case material. They often require that employees sign an annual FCPA statement stating that they understand the Act. This also documents that the company has been proactive in communicating that it will not tolerate improper business practices.

- **Provide mechanisms to report violations.** A comprehensive whistleblower and complaint-handling process ensures that employees have a confidential means of notifying the home office of improper behavior.

- **Monitor for compliance.** Auditors, compliance officers or ethics officers should have some formal involvement in overseeing foreign operations.

- **Respond quickly and appropriately to reported violations.** The worst thing an organization can do is to have suspicions raised and not properly respond to allegations. Not only is this a guaranteed way of running afoul of the regulators, it also sends a message down through the ranks that the company is not serious about punishing improper behavior.

At the first report of suspicious activity, the organization should conduct a prompt and thorough investigation. It may need to disclose certain information to the SEC, terminate employees, or even walk away from a
lucrative contract. Finally, the results of any investigation should be used to develop strategies for deterring future violations.

**Extending the Tone from the Top Beyond the Borders**

The due diligence required to comply with the FCPA may mean that, in some cases, U.S. companies in emerging markets will not be as competitive as businesses from other nations. If a government investigation does occur, a strong FCPA program will reduce the risk of criminal prosecution or civil sanctions because regulators will consider whether the business fostered an anti-bribery culture or one where violations could thrive.

In the U.S., Sarbanes-Oxley has placed companies on notice that intentional misrepresentation of their financial statements will not be tolerated. Thus, companies must remember that the importance of ethical and legal behavior does not stop when a company extends its operations overseas.

A common misperception is that when “no one is watching,” U.S. law does not apply. As the FCPA demonstrates, nothing could be further from the truth. Companies that believe otherwise do so at their own peril.
Antitrust investigations and lawsuits are rare; but once initiated, they can be costly and destructive to a gaming enterprise and its executives. Antitrust law seems simple—do not conspire and agree to restrain trade or attempt to monopolize a business. However, many companies run into problems, because they fail to recognize risky activities and implement effective antitrust compliance programs.

Those who run substantial businesses participate in trade associations or have friendly relations with competitors need to be careful. The entities and individuals who have gotten caught up in antitrust actions will almost surely attest that their experience was ugly, protracted, unusually expensive and difficult to defend. When violations are proven, the violators—whether corporations, their officers, or both—can be prosecuted criminally and a handful of examples are made of individual business people every year.

Most antitrust problems can be avoided by instituting and adhering to even a basic compliance program. One element of any compliance program should be to have a written antitrust compliance policy. Almost all Fortune 500 companies and trade associations have such policies, and several have gone so far as to publicize their policies.

Of course, written compliance policies accomplish nothing unless they are coupled with meaningful education about what is improper behavior. Notwithstanding the great complexity of antitrust law, nearly all business executives can, in a very brief time, learn antitrust law basics well enough to at least recognize the most dangerous situations. In fact, most companies are able to set forth the basics in their compliance policies, while still being able to keep their policies short enough to be useful.

**Enforcement, Litigation and Damages**

Antitrust laws are enforced by both federal and state regulators and prosecutors. At the federal level, both the Department of Justice and the Federal Trade Commission have jurisdiction over antitrust laws. Most
states also have their own antitrust laws, which generally (with some major exceptions) mirror federal law.

For example, the State of Nevada has the Unfair Trade Practices Act ("Act") covering prohibited antitrust activities. The Act lists prohibited antitrust conduct in an attempt to compile the more frequent practices deemed illegal under federal law. Nevada also has very specific antitrust statutes for the insurance, alcohol, auto financing, dairy and cable television industries. These laws are enforced by the Nevada Attorney General or, in some instances, local district attorneys.

Besides enforcement actions, private parties can also bring antitrust lawsuits against gaming companies and executives and, when the private parties win, they are awarded not only their damages, but three times their actual damages (because we supposedly want to encourage private parties to bring antitrust suits), plus their attorneys’ fees. Yet, despite the seeming incentives to bring such suits, for a variety of reasons, not that many suits are filed.

For those entities and individuals implicated in antitrust violations, the experience is likely to be protracted and expensive. Antitrust allegations are usually difficult to defend and harmful for business. In those cases where illegal antitrust activities are proven, companies and their officers face civil and criminal penalties.

**Antitrust Law Basics**

The primary federal antitrust law, the “Sherman Act,” was enacted in 1890 and is famous for how short and unspecific its two primary provisions are.

**Section 1**: “Every contract, combination … or conspiracy, in restraint of trade …. is hereby declared to be illegal.”

The important thing about Section 1 is that it only concerns agreements—i.e., arrangements between two or more parties. If anti-competitive acts are committed unilaterally, that is, absent an agreement or a “conspiracy” with another party or parties, it is not illegal under Section 1. In addition, because so many agreements to one degree or another restrain trade,
the Act was quickly interpreted to mean that only agreements that “unreasonably” restrain trade are illegal. Of course, that clarification can be broadly interpreted.

Here are a few of the most common illegal agreements under Section 1:

- **Price-Fixing.** Almost any arrangement (no matter how informal) between competitors where agreement is reached on the prices to be charged is illegal. Further, indirect arrangements may be illegal if their purpose or main effect is to eliminate full price competition between competitors.

- **Market or Customer Division.** Competitors (even if only potential competitors) cannot agree to divide up markets or customers. For example, “We’ll stay out of Reno if you’ll stay out of Las Vegas”; or, “We’ll not bid on Job X if you’ll not bid on Job Y.”

- **Concerted Refusals to Deal.** Sometimes businesses have a common problem; perhaps a supplier is overcharging or a customer’s demands are unfair. It might be tempting to agree to jointly boycott that supplier or customer to coerce them to make concessions. While tempting, such collusion might be illegal.

In summary, Section 1 of the Sherman Act is concerned with agreements that might disrupt competition. It does not cover unilateral decisions about pricing or marketing, no matter how aggressive.

**Section 2:** “[W]ho shall monopolize, or attempt to monopolize, or combine or conspire with any other person …. to monopolize” shall be committing an illegal act.

This section of the Sherman Act applies to the unilateral acts of a single entity, but only if that company has become a monopoly or is realistically attempting to become one. A “monopoly” acquired and maintained through legitimate business conduct (i.e., through superior business acumen, historical accident or intellectual property rights) is generally not included by this section of the Act.
However, in situations where a business has a very large market share of a definable market (say, over 65%), or would acquire such a share through a consolidation or merger, it has to be very careful about its conduct, lest aggressive business conduct that might be deemed acceptable for a small competitor is deemed to be improper monopolistic conduct.

Section 2 has particular applicability to:

- **Mergers and Acquisitions.** If two major players are ceasing to be competitors in a given market through a merger or acquisition, they typically must seek prior permission from regulators.

- **Predatory Pricing.** Although a difficult claim to prove, an enterprise having a high market share runs a risk for antitrust claims if it prices products or services fall below average variable costs to drive smaller competitors from the market.

- **Exclusive Dealing Arrangements.** Again, though a difficult claim to prove, an entity with a high market share runs a risk if it “ties up” a high percentage of the market’s major customers or suppliers for extended periods through exclusive dealing contracts—i.e., contracts that require the customers or suppliers to purchase or sell to that party only.

Obviously, Section 2 has zero applicability to the vast majority of businesses—very few businesses are a monopoly or on the verge of becoming one.

**Where Problems Happen**

Some antitrust conspiracies are hatched at the highest levels. And when those conspiracies are revealed, the punishment can be spectacular. For example, manufacturers of vitamins met in the Black Forest of Germany in the early 1990s to fix vitamin prices and divide up markets. The Department of Justice ultimately uncovered the conspiracy and F. Hoffman La-Roche, Ltd. agreed to pay a $500 million fine. In many such high-profile cases, individual officers have been indicted.

But cases where the misconduct is hatched and carried out at the senior executive level of large corporations are rare. Far more common are cases
where a company finds itself not so much “caught” committing an obvious antitrust violation, but instead “caught up” in a suit or investigation based on unauthorized conduct by a small handful of people at the company. While most antitrust misconduct requires the existence of an “agreement,” executives must keep in mind that the agreement requirement is construed broadly by regulators and courts. Stereotypical backroom conspiracies are in no way required for an appearance of misconduct to exist.

One typical risk involves the sales force. At most sales organizations, sales persons talk to each other, and competitors, about products and pricing. Occasionally, this leads to information sharing and informal agreements to fix prices or split up customers or markets. Interpreted loosely, these arrangements may cross the line into conspiracy and violate antitrust laws. Similarly, while trade associations serve many useful functions, employee participation in trade association activities may also inadvertently create risks for antitrust claims. Whenever competitors gather, there are obvious opportunities for collusion. Stray, inappropriate comments are common in this setting. Even in cases where no actual collusion occurs, the seemingly harmless, albeit inappropriate, comments have been misconstrued, causing inquiries and allegations. If there is ever cause for an investigation about what was said at association meetings, such comments may be attributed significance that they perhaps do not deserve. Therefore, companies whose employees participate in trade associations must educate those employees about proper conduct in that forum, a task that can be handled largely in a compliance policy that contains guidelines about trade association participation.

Finally, companies have to be cautious when terminating suppliers or distributors. While recent court rulings indicate antitrust cases brought by terminated suppliers or distributors rarely succeed, such cases are commonly brought and can prove highly embarrassing, expensive and, occasionally, an antitrust problem. For example, there may be every right contractually to terminate a distributor, but if there are internal e-mails indicating that the distributor was being terminated because of its pricing
policies, or its willingness to work with a competitor, a prolonged lawsuit experience may be needlessly created.

**Compliance Programs**

Most antitrust problems are avoidable by instituting and adhering to a basic compliance program. Good compliance programs have, at their heart, a written compliance policy that is widely disseminated and that is actively referenced; obviously, another policy put into a notebook that is sent out one time as an attachment to an e-mail is not going to accomplish this. Written compliance policies are enhanced when coupled with education and the reinforcement of proper behavior.

Antitrust compliance policies need to be tailored based on the size and complexity of the gaming company. Complete policies have these attributes:

- **Acceptable Actions:** A list and description of allowable conduct approval requirements for specified activities. For example, employees should be expressly cautioned about discussing pricing or other sensitive marketing terms with competitors.

- **Reporting:** Describe reportable actions together with the process and chain of command for reporting suspected violations. This includes policies dealing with whistleblowers and anonymous reports. For example, an employee may become concerned not because of his or her conduct, but rather because of an inappropriate statement made to that employee by a competitor. The policy should make clear that ANY issues of concern should be reported, and it should identify to whom that report should be made.

- **Recordkeeping:** Record retention policies for antitrust risks should be consistent with other business records policies. For example, employees should be cautioned that it is inappropriate to destroy documents, e-mail or other records when directed to do so by others if they believe the motivation may be to conceal antitrust misconduct.
• **Internal Privacy:** Compliance policies should require confidentiality of sensitive information. For example, proprietary information, unsubstantiated claims, accused parties and sources of information should be kept confidential for management and company officials to handle. Compliance policies also should endeavor to set up reporting mechanisms where the identity of a person making a report will be, to the extent possible, kept confidential.

**Education is the Best Protection**

Antitrust claims are serious; they relate to a conspiracy and agreement to restrain trade or monopolize business. However, the risks associated with antitrust can be successfully managed.

The best protection is educated personnel, who can monitor not only their own and their co-workers’ behavior, but perhaps be in a position to spot a potential problem before it becomes a real one. Indeed, companies with employees who understand the antitrust laws are far more likely to recognize when the company is being victimized by antitrust misconduct of others. Compliance policies with provisions regarding acceptable behavior, reporting, recordkeeping, and privacy are the foundation for compliance. Such policies, taught to all personnel and reinforced regularly, reduce exposure to illegal antitrust activities. In fact, under federal sentencing law, companies convicted of an antitrust violation, but which had a bona fide compliance program in place, are to be treated considerably more leniently than companies without such programs.
Chapter 15
ADVERTISING AND MARKETING: KEEP IT COMPLIANT

Compliance plans and advertising seem like strange bedfellows. After all, what advertisements can possibly cause gaming regulatory compliance issues? One Las Vegas casino attracted the unwanted attention of gaming regulators when it embarked on a risqué series of billboards. One showed cards, poker chips and a couple in a suggestive pose with the tagline: “There’s always a temptation to cheat.” Another declared that the casino supported “your Monday night rights: large quantities of prescription stimulants, having wives in two states ... Tell your wives you are going; if they are hot, bring them along.” Nevada’s gaming regulators decided that illicit sex, illegal drugs and casino cheating were over the top even for Las Vegas and brought a complaint alleging a violation of Nevada Gaming Regulation 5.011(4) that sanctioned the casino for a “Failure to conduct advertising and public relations activities in accordance with decency, dignity, good taste, honesty and inoffensiveness...” The casino ultimately agreed to pay a fine of $300,000 and implement new compliance procedures to review future advertisements. While the Nevada Gaming Commission ultimately decided to reject two of the three counts in the final decision because of First Amendment questions, such conflicts can strain relationships with the regulators and the community.

Other advertising issues do not invoke Constitutional considerations. Even the ardent civil rights lawyer will acknowledge that the Constitution offers no protection against false or misleading advertisements. Both gaming regulatory laws and general consumer protection laws provide sanctions, both criminal and civil, for such advertisements. The same Nevada regulation cited above prohibits “advertising that is false or materially misleading.” California has a statute that criminalizes advertising that concerns “any circumstance or matter of fact connected with the proposed performance or disposition thereof, which is untrue or misleading, and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading.” Frequent occurrences that raise the interest of regulators are quantifiable claims that are simply untrue. For example, a casino cannot
advertise that it has the loosest slot machines in town unless they can show by some reasonable standard their slot machines have the highest average return.

A casino also can get into trouble not by what it says in advertisements, but what it does not say. Some states, like New Jersey, require all casino advertisements to provide information regarding compulsive gambling programs, including providing an 800 number.

Finally, a casino can violate gaming regulations and other laws by sending casino advertisements to prohibited groups. Well-known Michigan gaming attorney Robert Stocker issued this warning to the Michigan gaming industry: “On August 10, 2006, the Michigan Attorney General filed criminal and civil charges against two senders of unsolicited messages to minors whose e-mail addresses were registered under the Michigan Child Protection Registry Act. The Michigan Act declares that it is the Legislature’s intent ‘to provide safeguards to prevent certain messages regarding …. gambling …. from reaching minor children of this state.’ In reality, the Michigan Act exposes the gaming industry to criminal and civil prosecution for a wide variety of lawful commercial business activities.” Minors are not the only group protected from casino advertisements. In New Jersey, for example, problem gamblers can request to be placed on the list of self-excluded persons. Once on these lists, casinos should not send these individuals any forms of casino-related advertising or offer them any casino-related benefits.

Advertising is not the only form of communications that can lead to regulatory problems. Gaming companies have faced stiff fines for public relations that have gone astray. In one recent case, the Nevada Gaming Commission fined a manufacturer for issuing a press release that claimed it entered into a contract with another party when it had only entered into a letter of intent that was never consummated. False or misleading financial press releases pose an additional risk of civil law suits and sizable money damages. For example, in 2006, Time Warner settled a case with the Pennsylvania Public School Employees’ Retirement System and others
for $23 million for false and misleading statements concerning the business, financial results, and operating condition of Time Warner.

Compliance committees, however, are not well equipped to review every press release or advertisement for proper content or to scrutinize the mailing lists for such advertisements. The compliance plan, however, can recognize the potential problems that can occur with both advertisements and public relations. The plan should inform company employees of their obligations regarding appropriate advertising, describing and warning personnel of the dangers of false or misleading advertisements or press releases. The plan should provide systematic policies for review of all advertisements and press releases by the respective company personnel and outside advisers. A company may require the chief financial officer and corporate legal counsel to review all press releases before they are issued. The compliance officer also may review advertisements before publication. Policies can be implemented to require that e-mail lists be regularly compared to the rolls of states with Child Protection Registry laws to ensure that advertisements do not inadvertently reach minors on the list. Likewise, all advertisement lists can be checked against any state lists of excluded persons and purged appropriately to avoid regulatory violations.
In the wake of the Enron scandal that rocked the public company sector, Rod Smith, a reporter for Casino City Times, questioned why the gaming industry had not experienced similar problems. Terry Lanni, then MGM Mirage Chairman and CEO, had a simple explanation: “We’re a highly regulated business. Therefore, any partnerships (involving conflicts of interest) would be impossible to occur in this business. Clearly, any such event such as those in Enron would have been impossible (in the gaming industry).” Likewise, Steve Crown, compliance committee chairman at Park Place Entertainment Corp., noted: “From a compliance perspective, we’ve become our own watchdogs.” Mr. Crown continued, “What saved the gaming industry from the financial turmoil that enveloped other industries was stringent adherence to compliance policies that prevent ‘conflicts of interest.’”

A conflict of interest arises when a person has two duties that conflict, or, more specifically, Black’s Law Dictionary defines it as “a real or seeming incompatibility between one’s private interests and one’s public or fiduciary duties.” In the corporate context, for example, a conflict of interest exists if an employee has a direct or indirect pecuniary or personal interest in a decision being made that needs to be made objectively and in the best interests of only the company. However, the occurrence of conflicts of interest does not necessarily signify impropriety, especially considering that conflicts can arise in everyday life.

Although all conflicts may not be unethical or improper, the heightened state of today’s corporate regulatory environment demands companies implement and enforce industry specific compliance plans designed to safeguard against the negative implications conflicts of interest may give rise to at all levels of the corporate structure. A post-Sarbanes Oxley American Bar Association course listed five key areas compliance plans
should address: (1) assigning responsibility for overseeing compliance to a high-level employee; (2) communicating the compliance plan standards and procedures to all employees through training, written communication, or any other means; (3) instituting monitoring and reporting systems to detect unauthorized conduct, enable employees to report unauthorized conduct, and report such conduct to the high-level employees overseeing compliance; (4) effectively enforcing the compliance plan; and (5) ensuring internal corporate disciplinary and remedial actions for employee violations.

A carefully tailored compliance plan will serve as an invaluable guide for a company, because it will assist a company in navigating the myriad of federal, state and local laws affecting its business. Additionally, the plan will provide both ethical and legal guidance to ensure employees act free of any conflicts and carry out their duties and responsibilities in the best interests of the company. Most notably, a well envisioned compliance plan will inform employees of likely pitfalls, institute disciplinary and remedial actions for compliance violations, and implement an approval process for certain actions. These procedures enable companies to effectively vet potential conflicts. Such foresight lays the foundation for an educated and unbiased workforce.

States have passed or enacted conflict of interest statutes and regulations recognizing a need for conflicts of interest oversight. With respect to the gaming industry, states have adopted conflict of interest laws regulating how state employees may interact with gaming licensees. For example, the Nevada Revised Statutes state, “[A] person who holds a license issued pursuant to chapter 463 or 464 of NRS or who is required to register with the Nevada Gaming Commission pursuant to chapter 463 of NRS shall not employ a former member of the State Gaming Control Board or the Nevada Gaming Commission for one year after the termination of the member’s service on the Board or Commission.”

The rationale for these policies is compelling: control employee behavior to both bolster regulatory compliance and limit possible violations that could otherwise result in severe financial penalties and subject the company to critical licensing issues, while assuring that corporate resources are not
Getting in the Game: A Guide to Successful Gaming Compliance

squandered through employee self dealing. Therefore, to adequately educate and yield beneficial results, these written policies should not only set forth the objectives of the policy but also the reasons for it.

**Details to include in your Compliance Plan**

Many conflicts of interest can be avoided through appropriately designed compliance controls. In such a highly regulated industry as gaming, perhaps the foremost concern is to avoid all conflicts of interest that would reflect poorly upon a gaming organization’s standing with the regulators and could thereby jeopardize its gaming license. This includes ensuring all employees are aware of acts and situations that i) are improper; ii) might give an appearance of impropriety; or iii) might impair their good judgment when acting on behalf of the company.

In particular, potential situations that would give rise to conflicts of interest should be detailed in a compliance plan. These situations include, among others:

- Having a significant interest in a firm that does business with the company.
- Borrowing or accepting money or gifts or other favors from a person or firm doing business with the company.
- Engaging in a private business relationship with a person or firm doing business with the company, particularly if the company’s employee supervises the relationship with that person or firm.
- Engaging in a private business relationship with a supervisor or another team member whom the team member supervises.
- Engaging in a competing business or owning stock or other securities of a competitor other than insignificant interests in public companies.
- Engaging in a private business venture with an officer or other employee of a firm that competes with the company.
• Using company resources for personal benefit, such as the extension of complimentary items or services, to further personal rather than a company business purpose.

• Use of company staff or assets for personal business.

• Having an interest in or speculating in products or real estate whose value may be affected by the company’s business.

• Improperly divulging or using confidential information such as plans, operating or financial data or computer programs.

• Indirect conflicts of interest such as transactions involving a spouse, children or other close relative (dependent or independent) or business associate.

Because conflicts of interest will arise as a matter of course, a company should adopt a compliance plan with internal controls to identify and report conflicts. This should include procedures enabling employees to report these conflicts, and a subsequent review process to determine whether the conflict requires intervention or can exist without detriment to the company. Adherence to such a plan enables a company to ensure regulatory compliance while providing employees with the knowledge that their relationships do not conflict with their duties to the company.

**Laws**

When implementing internal controls for conflicts of interest, companies must also ensure those controls comply with any restraints imposed by state conflict of interest laws. Most notably, this includes compliance with those state conflict of interest laws specifically designed for the gaming industry. For example, both New Jersey and Colorado gaming licensees must comply with multiple government-imposed mandates.

New Jersey Conflicts of Interest Law controls licensee conduct in numerous situations, including prohibiting a licensee from employing state employees who were responsible for casino matters within two years of termination from state employment. Additionally, the New Jersey Casino Control Act regulates political conflicts of interest originating from licensees, one
example of which is to prohibit licensees and their agents from making political donations.

Colorado’s Limited Gaming Act and Gaming Regulations control similar conflicts of interest situations. For instance, licensees and their agents are prohibited from giving anything of value to Colorado Limited Gaming Control Commission members and their close relatives or from allowing Commission members and their close relatives from having interests in their casino license. Furthermore, licensees and their agents are prohibited from allowing Commission employees to participate in any gaming authorized by the state and operated by the licensee.
Noticing the organic unification of financial markets in our globalized economy, for a long time, has fostered an environment well-suited to money laundering and terrorist financing. While in the post-9/11 world, domestic and international entities have made great strides working together to combat the threat money laundering poses to the global economy, international inconsistencies in legal structures and the complexity of the domestic regulatory environment continue to pose challenges to these efforts. Compounding this situation within the anti-money laundering (AML) community is the current global financial crisis, which has wreaked havoc on financial markets and institutions across the globe.

The crisis obviously takes priority over compliance needs; however, the threat that money laundering poses to our global financial system, particularly in times of such economic instability, must not be ignored. In the seven years since the passage of the USA PATRIOT Act (the Patriot Act), the global financial system has made great strides not only in increasing awareness of money laundering, but also in providing a strong framework for combating it. Given the substantial momentum in global policy unification provided by international organizations, as well as movement toward consistent application of regulations domestically, the importance of AML compliance needs to be on the minds of management and boards now more than ever.

**Advances of International Member Groups**

International member groups such as the Financial Action Task Force (FATF) and the Egmont Group of financial intelligence units (FIU) have made great strides in recent years and have become recognized as international thought leaders within the AML community. Throughout its almost 20-year history, the FATF has worked to provide national and international policies to combat money laundering and terrorist financing to its members and the global community. In establishing its Non-Cooperating Countries and Territories (NCCT) list, FATF helped compile one of the only known, published lists of governments that did not conform to the 40 recommendations provided...
by FATF for sound AML regimes. This list, which at first included numerous countries and territories, ceased to exist after Myanmar—the last remaining country—was delisted by FATF in October 2007.

FATF recently has turned its attention from recommending policy on the general structure of an AML regime to closing the gap on outstanding AML issues that still have wide disparity internationally. These include the role of legal professionals in the fight against money laundering, as well as developing a risk-based approach for casinos to combat money laundering.

In June 2006, the plenary session of the Egmont Group met in Cyprus to discuss sending Egmont representatives to work with Interpol and Wolfsburg Group. Furthermore, Egmont Committee members met with representatives of FATF-Style Regional Bodies (FSRBs) to help determine the roles and responsibilities of various agencies in combating money laundering and terrorist financing. All these advances highlight that international unity is needed—and ultimately can be effective—to combat money laundering and terrorist financing.

**Fostering a Unified Framework for Combating Money Laundering**

Within the United States, interagency cooperation has helped foster a framework for a more unified front in combating money laundering and terrorist financing. In 2006, the Money Laundering Threat Assessment (MLTA) was produced by cooperating institutions consisting of experts from numerous U.S. Government agencies, bureaus and offices. The MLTA is a report that assists policy makers and regulators in understanding the current state of money laundering and offers tips to assist financial institutions in combating money laundering and terrorist financing. Besides helping policy makers, regulators and financial institutions combat money laundering and terrorist financing, MLTA also assists examiners of compliance programs to ensure that financial institutions’ anti-money laundering programs are functioning as they should be.

The Federal Financial Institutions Examination Council (FFIEC) released a second revision to the Bank Secrecy Act/Anti-Money Laundering Examination Manual in July 2007. This manual is used by examiners to ensure
that their clients’ AML compliance programs are working as they should, and helps protect the financial institutions, as well as their customers and stakeholders from fines and penalties.

Efforts to Streamline Regulatory Complexity Hurdles

In spite of major advances in the unification of policies globally and at home, regulatory complexity in the United States is still an issue. To address the regulatory challenges, the Financial Crimes Enforcement Network (FinCEN), the organization with the U.S. Treasury Department that administers the Bank Secrecy Act (BSA) and acts as the Treasury’s financial intelligence unit, has implemented a new initiative under the leadership of Director James H. Freis, Jr. to improve regulatory efficiency and effectiveness. This initiative has a two-fold approach: to provide a review of the regulatory framework with a focus on ensuring that requirements on covered financial industries are efficient in their application; yet, at the same time, to remain extremely effective in their service to law enforcement investigators, FinCEN analysts and regulatory examiners, who are tasked with safeguarding the financial system from the abuses of terrorist financing, money laundering and other financial crimes.

In October 2008, as part of this initiative, FinCEN proposed to simplify its rules and regulations by centralizing them in its own new chapter of the Code of Federal Regulations (CFR). The proposal would streamline the BSA regulations into general and industry-specific parts, ensuring that a financial institution will be able to identify its obligations under the BSA in a more organized manner.

AML Compliance Requirements Vary by Industry

Despite FinCENs best efforts, industries subject to the Bank Secrecy Act as amended by the Patriot Act are faced with uneven regulatory requirements. Banks and other deposit institutions have long been examined and reviewed for AML compliance and, as the first institutions to be targeted to ensure compliance, have been able to provide a solid AML approach. Likewise, Money Services Businesses (MSBs) have been faced with a high level of scrutiny due to their inherent risk and have been able to develop the necessary compliance programs.
On the other hand, organizations such as insurance companies, although covered by the Patriot Act in 2001, did not face AML program requirements until 2006. At this point, the IRS has begun to conduct examinations of the larger players in this industry, but has not made a complete pass at ensuring compliance for all organizations. Since compliance program development and examinations are extremely new, undoubtedly there will be growing pains in policy adoption by companies, as well in implementation of consistent examination strategies by the IRS.

The Four Pillars of an Effective AML Compliance Program

To begin complying with government standards, institutions across industries, at the minimum, should apply the four pillars of the AML program. These four pillars are as follows:

- Develop policies for preventing the institution from being used to launder money and for dealing with cash and monetary instruments.
- Designate a compliance officer to implement the anti-laundering program.
- Establish a training program for all areas subject to laundering.
- Establish an independent test/audit function that reviews and tests activities into specific accounts.

While these four pillars are a starting point, organizations must take compliance a step further. They must become keenly aware of their gaming industry regulatory requirements and continually be vigilant not only in ensuring regulatory compliance, but also in keeping their organization safe from the threats of money laundering and terrorist financing.

This financial crisis will no doubt take resources away from efforts such as AML compliance, but—given the momentum of recent years’ advances in combating money laundering—now is the time when compliance efforts must be on the forefront of the minds of directors, officers, and management in the gaming industry.
As you can see from the examples illustrated in this publication, it is vital for companies in the gaming industry to develop a comprehensive compliance plan that is well communicated to its employees, board members, and committee members to avoid potential compliance and regulatory issues and unethical practices. As with all businesses, a strong compliance culture has never been more important. Compliance failure poses a serious threat to any company’s reputation which if tarnished, can be difficult to overcome. In the gaming industry, these infractions can carry significantly higher consequences resulting in the risk that literally may mean “all bets are off.”
LEWIS AND ROCA, LLP

Lewis and Roca is one of the Southwest’s leading law firms. Founded in 1950, with over 200 attorneys in offices in Las Vegas, Reno, Phoenix, Tucson, Albuquerque and in the Silicon Valley, our firm serves a diverse base of local, national and international clients. Lewis and Roca’s gaming practice supports casino operators, suppliers, equipment manufacturers, state, local and tribal governments, businesses, non-profit organizations and others in addressing today’s gaming law issues. The gaming lawyers at Lewis and Roca have been at the forefront of all of the major emerging gaming trends including regulatory and licensing work for traditional casinos, Native American casinos, riverboat casinos, racinos, sweepstakes and Internet gaming. To learn more about our firm and the services we provide, please visit our website at www.LRLaw.com.

GRANT THORNTON, LLP

The people in the independent firms of Grant Thornton International Ltd provide personalized attention and the highest quality service to public and private clients in more than 100 countries. Grant Thornton LLP is the U.S. member firm of Grant Thornton International Ltd, one of the six global audit, tax and advisory organizations. Grant Thornton International Ltd and its member firms are not a worldwide partnership, as each member firm is a separate and distinct legal entity. To learn more, please visit our website at www.grantthornton.com.