

The SAR Activity Review *Trends Tips & Issues*

Issue 17

In focus: The Casino and Gaming Industry
Published under the auspices of the BSA Advisory Group.
May 2010



The
SAR
Activity
Review
Trends
Tips &
Issues

Issue 17

Published under the auspices of the BSA Advisory Group.
May 2010

Table of Contents

Introduction	1
Section 1 – Director’s Forum	3
Section 2 – Trends & Analysis	5
An Assessment of Suspicious Activity Reports Filed by Casinos and Card Clubs.....	5
Analysis of Inquiries from Casinos and Card Clubs Regarding Suspicious Activity Reporting Requirements.....	15
How Examiners Use BSA Data to Scope and Plan Casino Examinations.....	19
<i>The SAR Activity Review – By the Numbers</i> as a Resource.....	22
Section 3 – Law Enforcement Cases	32
Section 4 – Issues & Guidance	44
Suggested Best Practices – Casino or Card Club Risk-Based Compliance Indicators.....	44
Casino or Card Club Compliance Assessment.....	50
Section 5 – Industry Forum	56
Anti-Money Laundering (AML) Programs and Nevada’s Casino Industry – Training and the Methods Used for Detection of Money Laundering and Fraud.....	56
Bank Secrecy Act Compliance Challenges in an Environment of Declining Revenue.....	63
Section 6 – Feedback Form	66

The SAR Activity Review **Index** is now available on the FinCEN website at:

http://www.fincen.gov/news_room/rp/files/reg_sar_index.html

For your convenience, topics are indexed alphabetically by subject matter.

The **Archive of Law Enforcement Cases** published in *The SAR Activity Review* can be accessed through the following link:

http://www.fincen.gov/news_room/rp/sar_case_example.html

Introduction

The *SAR Activity Review – Trends, Tips & Issues* is a product of continuing dialogue and close collaboration among the nation’s financial institutions, law enforcement officials, and regulatory agencies to provide meaningful information about the preparation, use, and value of Suspicious Activity Reports (SARs) and other Bank Secrecy Act (BSA) reports filed by financial institutions.

This edition focuses on the casino and gaming industry, but also addresses several noteworthy topics that relate to other industries. Articles in the *Trends & Analysis* section include an assessment of SARs filed by casinos and card clubs by FinCEN’s Office of Regulatory Analysis (ORA) as well as an analysis of casino calls to the Regulatory Helpline by FinCEN’s Office of Outreach Resources. An article by staff of the Internal Revenue Service (IRS) explains how casino examiners use BSA information. Finally, ORA provides an overview of how the companion piece to this publication, *The SAR Activity Review – By the Numbers*, can be used as a valuable resource by a variety of stakeholders.

As always, the law enforcement cases in Section 3 demonstrate how important and valuable BSA data is to the law enforcement community. This section focuses on cases where defendants either pled guilty or were convicted at trial on BSA-related violations. In the *Issues & Guidance* section, we provide suggested best practices for casino or card club risk-based compliance indicators as well as for performing a risk-based compliance assessment. In the *Industry Forum* section, we show an industry viewpoint on training and the methods used for detection of money laundering and fraud. We also provide industry view of BSA compliance challenges in an environment of declining revenue.

The SAR Activity Review is possible only as a result of the extraordinary work of many FinCEN employees and FinCEN’s regulatory, law enforcement and industry partners. In order to recognize their hard work, we acknowledge contributors throughout the Review.

You can subscribe to **FinCEN Updates** under “What’s New” on the FinCEN website, www.fincen.gov to receive notification of when *The SAR Activity Review* is published. As always, your comments and feedback are important to us. We have included a feedback form in Section 6; please take a moment to let us know if the topics chosen for this issue are helpful as well as any other suggestions or comments you might have about *The SAR Activity Review*.

Your comments may also be addressed to either or both of *The SAR Activity Review* project co-chairs:

Lilly Thomas
Regulatory Counsel
Independent Community Bankers of America
1615 L Street, NW, Suite 900
Washington, DC 20036-5623
Phone: 202-821-4409
lilly.thomas@icba.org
www.icba.org

Sean Smith
Regulatory Outreach Project Officer
Financial Crimes Enforcement Network (FinCEN)
PO Box 39
Vienna, VA 22183
Phone: 202-354-6400
sar.review@fincen.gov

Please do not submit questions regarding suspicious activity reports to The SAR Activity Review mailbox.

Section 1 — Director's Forum



This year FinCEN is commemorating its 20th Anniversary. I hope you will take a moment to join me in reflecting upon how far we — as a partnership between financial institutions, law enforcement agencies, and State and Federal regulators — have progressed in the last two decades. FinCEN was created to be the bridge between law enforcement agencies and the financial industry. Our prescient designers saw the need for a central repository of financial intelligence that would collect, protect, and analyze the valuable information that industry could provide and then share it with law enforcement

agencies, which at the time were holding several disparate and unconnected databases of their own. At the time a novel concept, the connections that FinCEN made, and the investigatory efficiency it provided, allowed users of the data to avoid duplicative efforts and to target their resources more effectively.

FinCEN began in 1990 with an assemblage of financial crime and technology experts drawn from the then-U.S. Customs Services (USCS), the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), the IRS, and elsewhere. Reports then required under the BSA, mainly Currency Transaction Reports (CTRs) and associated criminal referral forms, gave FinCEN the rudimentary tools to begin its operations. With the advent of Suspicious Activity Reports (SARs) in 1996, the international responsibilities that came with the establishment of the Egmont Group in 1995, the expansion of covered financial industries and counter-terrorist finance mission brought about by the USA PATRIOT Act in 2001, the amount of financial intelligence available for analysis and sharing and FinCEN's role has increased dramatically.

The financial world of 1990 was very different from today. Financial assets of banking institutions have increased from \$3.3 trillion in 1990 to over \$13 trillion in 2008. In 1997, depository institutions filed 81,000 SARs, and in 2009, they filed over 720,000. Over the years, Money Services Businesses (MSBs), Securities and Futures firms, Insurance Companies, Mutual Funds, and Casinos (the subject of a more in-depth study in this edition of *The SAR Activity Review*) have collectively provided over 3 million more.

During the past twenty years, FinCEN has acquired greater regulatory authority, additional responsibility for more covered industries, a significant international role, and greater information technology demands. Its staff has grown from about 200 to its current strength of 327 full-time employees. The crucial role that FinCEN plays in safeguarding the financial system is well accepted.

There is no longer any question about the value of CTRs in fighting financial crime. As more than 100 SAR review teams located around the country and members of the Administration's Financial Fraud Enforcement Task Force can attest, SARs continue to be among the best sources of lead information in developing mortgage fraud and other financial crime cases.

With those thoughts in mind, I welcome you to this 17th edition of the *Review*. Although the general public might not consider a casino to be a "financial institution", they are businesses involved in the movement of a lot of money and it is essential to include the casino and card club industry in our efforts to prevent criminal abuse. This *Review*, focusing on the casino industry, is the latest in a range of recent publications we have put out to raise awareness and compliance throughout the casino industry. State-licensed casinos were made subject to the BSA in 1985. At the time only two states allowed casinos. Since then the number has grown to more than forty states and many additional tribal casinos. Within these pages you will find an assessment of SARs filed by casinos, suggestions for best practices, and other useful information for the industry.

FinCEN continues to assess and adjust its rules and guidance for casinos. The final rule which amended the filing requirements for Casino CTRs (CTR-C) was the first one which we subjected to our policy of an 18-month review. This review was to objectively gauge the impact of our rulemaking efforts. The reasoning behind the rule change was that slot machine jackpots in excess of \$10,000 are not likely to be part of a scheme to launder funds. We found that our rule resulted in a 35 percent decrease in CTR-Cs and that decrease allows casinos to focus on the SARs and CTR-Cs that are truly useful to law enforcement.

As always, you will find additional law enforcement case examples that illustrate the use of SARs in criminal investigations, and we continue to welcome your feedback concerning this publication and encourage your use of our regulatory helpline.

James H. Freis, Jr.
Director
Financial Crimes Enforcement Network

Section 2 - Trends & Analysis

This section of *The SAR Activity Review - Trends, Tips & Issues* focuses on the BSA reporting patterns of the casino and gaming industry. This section also contains an analysis of casino and card club industry inquiries received by FinCEN's Regulatory Helpline. Finally, this edition of *The SAR Activity Review* highlights the value of a companion publication, *The SAR Activity Review – By the Numbers*.

An Assessment of Suspicious Activity Reports filed by Casinos and Card Clubs *By FinCEN's Office of Regulatory Analysis*

The BSA and its implementing regulations define a gaming casino as a financial institution subject to the BSA requirements if it (1) has gross annual gaming revenue of more than \$1 million; and (2) is duly licensed as a casino under the laws of a State, territory or possession of the United States; or if it is a tribal gaming operation conducted pursuant to the Indian Gaming Regulatory Act (IGRA)¹ or other Federal, State, or tribal law or arrangement affecting Indian lands, including casinos operating under the assumption or under the view that no such authorization is required for casino operation on Indian lands.² For example, tribal gaming establishments that offer slot machines, video lottery terminals, or table games,³ and that have gross annual gaming revenue in excess of \$1 million, are covered by the definitions. The definition applies to both land-based and riverboat operations licensed or authorized under the laws of a State, territory,⁴ or

1. The Indian Gaming Regulatory Act is codified at 25 U.S.C. § 2701 et seq.
2. See 31 CFR § 103.11(n)(5)(i).
3. Slot machines, video lottery terminals, and house-banked table games would qualify as Class III gaming under the Indian Gaming Regulatory Act. Bingo and related games, including pull tabs, lotto, punch boards, tip jars, instant bingo and some card games, would qualify as Class II gaming under the Indian Gaming Regulatory Act.
4. This includes casinos located in Commonwealth of Puerto Rico, St. Croix (U.S. Virgin Islands), and Tinian (Northern Mariana Islands). See 31 CFR § 103.11(tt).

tribal jurisdiction, or under the IGRA. Card clubs generally are subject to the same rules as casinos, unless a different treatment for card clubs is explicitly stated in 31 CFR § 103.

In addition to other requirements, 31 CFR § 103.21 requires casinos and card clubs to report conducted or attempted transactions or patterns of transactions that the establishment knows, suspects, or has reason to suspect are suspicious and involve or aggregate at least \$5,000 in funds or other assets.⁵ Since October 1997, Nevada casinos have been filing reports of suspicious activities under the State's previous regulatory system.⁶ Effective March 25, 2003, gaming establishments (including State-licensed operations, tribal casinos and card clubs) outside Nevada have been required to report suspicious transactions. The casinos and card clubs in Nevada and other jurisdictions had used FinCEN Form TD F 90-22.49, Suspicious Activity Report by Casinos and Card Clubs (SAR-C), which was replaced by FinCEN Form 102 effective April 1, 2003. Including both forms, from August 1, 1996 through December 31, 2009, casinos and card clubs filed approximately 62,193 suspicious activity reports.

This article is a statistical snapshot of SAR-Cs filed from 2004 through 2008; it summarizes the transactional trends and patterns that triggered the filings. A full assessment report will follow as a separate document.

Statistical Filing Trends

Using queries of the Document Control Number (DCN),⁷ FinCEN identified 40,409 SAR-Cs filed by casinos and cards clubs from January 1, 2004 through December 31, 2008. These SAR-Cs reported an aggregate of over \$900 million of suspicious activity. Although the SAR-Cs examined were filed from 2004 through 2008, some of the suspicious activity began as early as August 2001.

-
5. Financial institutions shall file with FinCEN to the extent and in the manner required a report of any suspicious transaction relevant to a possible violation of law or regulation. A financial institution may also file with FinCEN a Suspicious Activity Report with respect to any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by FinCEN regulations. *See, e.g.,* 31 CFR § 103.18(a).
 6. On March 20, 2003, the Nevada Gaming Commission deleted from its Regulation 6A all state requirements related to suspicious activity reporting. On March 25, 2003, all Nevada gaming operations meeting the definition of a casino pursuant to 31 CFR §103.11(n)(5) became subject to Federal suspicious activity reporting requirements.
 7. The DCN is an IRS-designated unique number assigned to each SAR-C submitted. It includes the date when the SAR-C was received and processed by IRS.

Overall, the annual number of SAR-C filings consistently increased during the study time period. The annual dollar amount of the filings, however, has fluctuated from year to year, at times decreasing. For example, while 15 percent of the 40,409 SAR-Cs in our study were filed in 2004, those filings accounted for 12 percent of the total dollar amount reported. In 2005, the percentage of SAR-Cs filed remained at 15 percent, but the percentage of the total dollar amount decreased to 8.5 percent. The last year of our review (2008) reflects the highest percentage of SAR-Cs filed (28 percent), and the percentage of the total dollar amount was nearly 28 percent - a percentage more than two times higher than in 2004. Table 1 summarizes the total annual filings and dollar amount involved in suspicious activity, and the corresponding percentage changes from year to year.

Table 1

Suspicious Activity Report by Casinos and Card Clubs (SAR-C) January 1, 2004 through December 31, 2008 Yearly Filings				
Filing Year	Filings	% Change From Previous Year	Reported Suspicious Amount	% Change in Amount From Previous Year
2004	5,962	0%	\$114,729,278 ⁸	0%
2005	6,072	2%	\$107,979,564	-6%
2006	7,270	20%	\$164,717,181	34%
2007	9,943	37%	\$279,475,643	41%
2008	11,162	12%	\$254,867,024	-10%
Total	40,409		\$921,106,353	

A breakdown of the filers by States/territories indicates that New Jersey casinos filed the highest number of SAR-Cs (26 percent), while Nevada ranked second on both highest number of filings (18 percent) and dollar amount reported (39 percent).

8. During 2004, it appears that a Mississippi casino filed erroneous amounts for 27 SAR-Cs totaling \$663,000,000 that should have been reported as \$663,000. The SAR-Cs contained various subject names pertaining to potential wire transfers, involving advance fee fraud schemes from five foreign countries that occurred during August 2003 and December 2004. The casino did not indicate that it had taken any additional action or suffered financial loss. Also, this Mississippi casino was unable to reconstruct its supporting documentation since it was destroyed by Hurricane Katrina in August 2005. Since *The SAR Activity Review, Trends Tips & Issues, Issue 7*, August 2004, indicates that in such a situation a SAR should not be filed, it would be reasonable to conclude that the 2004 total dollar amount should be adjusted downward from \$776,403,941 to \$114,066,941 to provide a more accurate picture.

Nine of the top ten filer states also appeared among the top ten states with the highest total dollar amount reported. Michigan is the exception since it ranked as the tenth top filer but did not appear among the top ten states with the highest dollar amount reported. Table 2 ranks the top ten filer states.

Table 2

Suspicious Activity Reports Filed by Casinos and Card Clubs (SAR-Cs)				
January 1, 2004 – December 31, 2008				
Top Ten Filer States				
Filer State	Total Filings	% of Total Filings	Total Dollar Amount	% of Total Dollar Amount
New Jersey	10,691	26%	\$195,715,587	22%
Nevada	7,097	18%	\$344,232,354	39%
Louisiana	2,753	7%	\$29,817,709	3%
Mississippi	2,454	6%	\$114,066,941	13%
California	2,408	6%	\$58,930,857	7%
Connecticut	2,383	6%	\$48,250,635	5%
Oklahoma	2,093	5%	\$20,999,715	2%
Indiana	1,893	5%	\$28,550,501	3%
Illinois	1,792	4%	\$35,693,372	4%
Michigan	924	2%	\$7,194,971	1%
Total	34,888	85%	\$883,452,642	100%

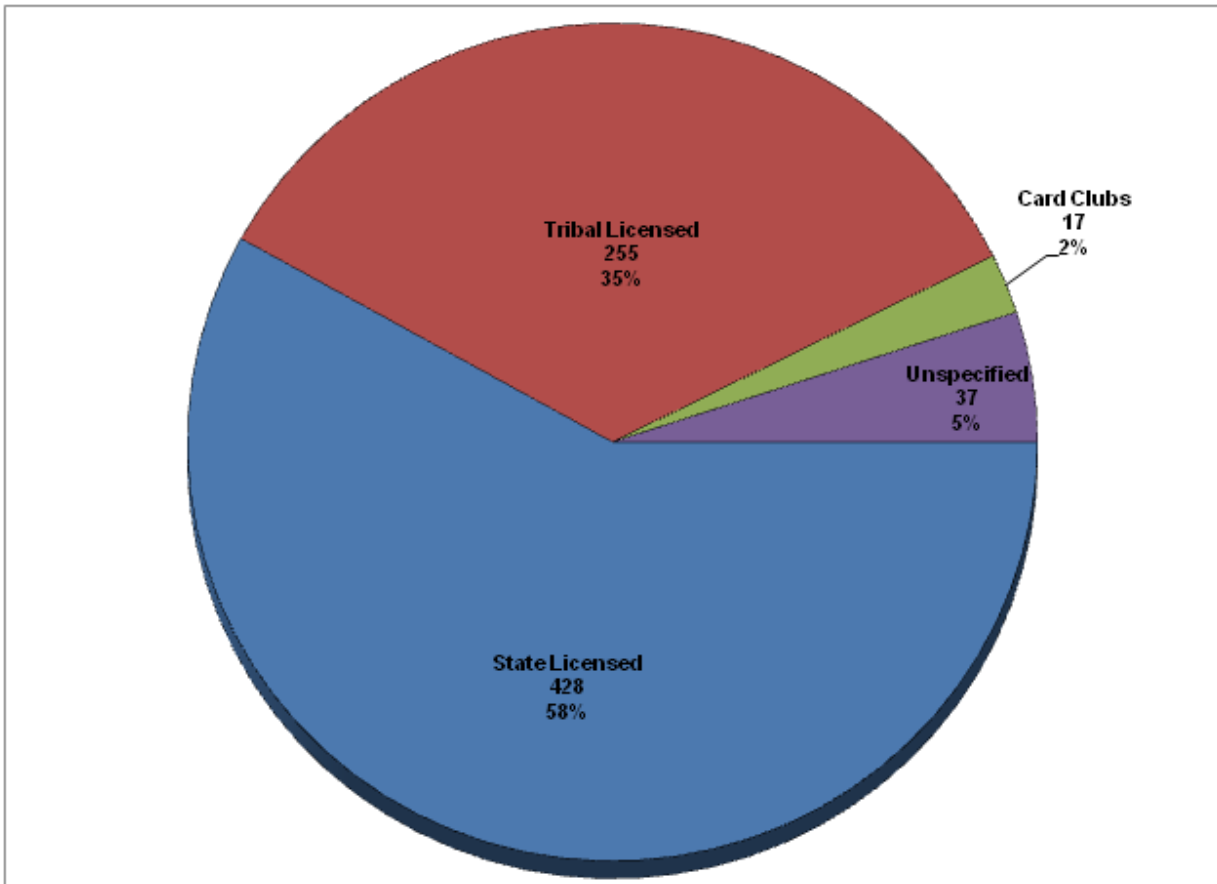
71 percent of the 40,409 SAR-Cs were filed by State licensed operations.

Table 3

Suspicious Activity Reports Filed by Casinos and Card Clubs				
January 1, 2004 – December 31, 2008				
Type of Gaming Institution				
Type of Gaming Institution	Total Filings	% of Total Filing	Reported Suspicious Amount	% of Reported Suspicious Amount
State Licensed (A)	28,761	71%	\$724,668,117	80%
Tribal Licensed (B)	10,316	26%	\$172,976,986	19%
Card Clubs (C)	362	1%	\$9,417,054	1%

The filers' Employer Identification Number (EIN) was included on 95 percent of the 40,409 SAR-Cs. Analysis identified 737 distinct EINs belonging to the various types of gaming institutions.

**Suspicious Activity Reports Filed by Casinos and Card Clubs
January 1, 2004 – December 31, 2008
Number of Distinct EINs per Type of Gaming Institution**



When characterizing the type of suspicious activity that they were reporting, filers reported "Structuring" in 32 percent of the total SAR-Cs, followed by "Other" (21 percent), and "Minimal Gaming with Large Transactions" (17 percent). An analysis of a sample of SAR-Cs that listed "Other" indicated that the suspicious activity probably should have been classified as "Structuring," "Minimal Gaming with Large Transactions," or "Check Fraud."

The individual suspicious activity amounts reported in the 40,409 filings ranged from \$1 to \$50 million. However, 40 percent of the total SAR-Cs provided suspicious activity amounts between \$10,001 and \$50,000.

Other key findings from the analysis follow.

- SAR-Cs filed within 30 days of detection: 95 percent
- SAR-Cs filed electronically: 76 percent
- SAR-C filers fully identified the subject(s) by listing the full name, address and a Social Security Number (SSN) on 59 percent of the SAR-Cs. Of the remaining SAR-Cs (41 percent), nearly half did not include a SSN but did list another type of identification such as a driver's license number, passport number, or alien registration number.⁹

What Triggered the SAR-Cs?

FinCEN analysts reviewed the narratives of 2,864 randomly-selected SAR-C reports and ascertained that the transactions, activities or behaviors that prompted the filings fall within several categories.

Structuring

Sixty percent of the sampled narratives reported individuals structuring or attempting to structure their transactions to avoid the filing of a CTR-C.¹⁰ Most of the structuring involved the cash out of chips, jackpots or checks followed by structured cash buys-in and payments on markers. Casinos detected most of the structuring at the time of the transaction, but some was identified later through reviews of internal files, such as the Multiple Transaction Log or the player's rating records. The key suspicious activities of patrons that casinos observed or detected and reported included:

- Reducing the number of chips or tokens to be cashed out at a cage when asked to provide identification or a SSN when the cash out was over \$10,000, or when a subject had previously cashed out chips or tokens and the additional cash out would exceed \$10,000 in a gaming day (the most reported structuring activity).
- Reducing the amount of cash buy-ins in pits to avoid providing identification or a SSN.

9. Nonetheless, of the total SAR-Cs filed during 2006 – 2009, over 8% did not contain any subject information (*i.e.*, full name, address, a SSN, or type of identification credential).

10. Federal law requires casinos and card clubs to report currency transactions over \$10,000 conducted by, or on behalf of, one person, as well as multiple currency transactions that aggregate to over \$10,000 in a single day. See 31 CFR § 103.22.

- Using agents to cash out chips: casino employees observed individuals handing over chips to agents to cash out. After cashing out the chips, agents were observed passing the cash to the true owners of the funds. Although many of the narratives identified at least the names of all the individuals involved, most listed only one individual in the SAR-C subject field (usually the true owner of the funds). A few filers opted to submit individual reports for each individual involved in the transaction.
- Cashing out chips, tickets, and/or tokens multiple times a day at different times or at different windows/cages: Several SAR-Cs reported individuals cashing checks multiple times a day but in amounts just below \$3,000 per location.
- Requesting jackpot winnings exceeding \$10,000 to be paid in two or three checks of lesser value.
- Depositing and withdrawing structured amounts of cash held in a safekeeping account.
- Wiring funds into front money accounts and depositing cash the next day followed by withdrawing half of the funds through structured drafts;
- Repaying outstanding balances with structured cash, wired funds, and checks over several days: One individual sent an agent on three different days to repay a debt with eight checks, all under \$10,000, drawn on the accounts of eight different companies at different depository institutions.
- Purchasing \$9,000 in chips with cash at the cage and purchasing another \$1,000 in chips with cash in a pit.

Minimal or No Casino Play

Thirty percent of the sampled narratives reported patrons conducting a series of transactions that involved minimal or no casino play.¹¹ Casinos identified patrons:

- Cashing out chips when the casino had no record of the individuals having bought or played with chips.

11. Minimal casino play most commonly refers to situations in which individuals exchange large amounts of currency for casino chips, gamble for a small amount of time (usually less than thirty minutes), either lose a nominal amount of chips or make small bets in comparison to the buy-in and then immediately cash out their chips. See Suspicious Activity Report Filings Within the Casino and Card Club Industries, [*SAR Activity Review, Trends, Tips and Issues, Issue 8*](#), April 2005, pages 13.

- Buying chips with cash, casino credit, credit card advances, wired funds or funds withdrawn from safekeeping accounts, but playing minimally or not playing at all. The subjects then cashed out the chips or left the casino with unredeemed chips.
- Receiving wired funds from a depository institution into an individual's casino front money account and then requesting that the funds be wired to a another bank account without playing: One subject had received weekly wire transfers during a 6-month period, played minimally and then cashed out the funds.
- Frequently depositing money orders or casino checks from other casinos into front money accounts, buying in and playing minimally, or not playing and then cashing out through issuance of a casino check.
- Converting currency into redeemable cash tickets by feeding bills (usually \$20s) into slot machine bill acceptors, and then printing out TITO tickets¹² and cashing out the tickets typically for large denomination bills.
- Exchanging small denomination bills for large denomination bills without playing.¹³

Misuse of Identification

Two percent of the reviewed sampled narratives reported subjects misused or attempted to misuse identification by providing false, expired, stolen or altered personal identifiers or identification credentials, mainly SSNs and drivers' licenses.

-
12. Slot machines or video lottery terminals allow customers to play on credits from bills, tickets or coins. The machines only dispense tickets and not coins. The Ticket in/Ticket Out (TITO) tickets, which can have any stated monetary value, can be inserted in an electronic gaming device that has the TITO function and can be played in such a device or cashed out with a cashier or at a kiosk machine.
 13. See FinCEN Educational Pamphlet on the Currency Transaction reporting Requirement at <http://www.fincen.gov/whatsnew/pdf/20090224.pdf>.

Fraud against the Casino

One percent of the sampled narratives indicated fraud or attempted fraud committed against the casinos through checks, counterfeit currency, advance fee scams or misuse of player's club points:

- Fraud through checks consisted of payments on markers typically with personal checks that were returned unpaid to a casino due to insufficient funds or accounts closed at depository institutions.
- Patrons cashed out or attempted to cash out stolen, forged or altered checks, as well as counterfeited \$20 and \$100 bills.
- Casinos received e-mails involving advance fee fraud schemes originating from several countries in South and West Africa which claimed to be seeking the casinos' assistance in arranging donations for a place of worship through a finance/security company in Europe, or seeking assistance in the transfer of large sums, in investment advice and in purchasing properties.
- A few SAR-Cs reported casino patrons who used their player club points to purchase significant amounts of U.S. gold eagle coins and/or gift certificates at an independently owned and operated retail store on the casino premises. Player points may be used to purchase goods and services at the casino's restaurants, retail shops or hotel. One individual reportedly converted gift certificates into cash using an agent for a retail store. Gold coins were reportedly converted into cash by using a third-party coin dealer. In some instances, the casino suspected that no coin or merchandise purchases actually occurred. Instead, filers said sham paper sale transactions were created and cash paid directly to the patrons for the player club points with the retail store in turn receiving monetary reimbursement from the casino for sales involving the use of player club points. The casino believed that officers and employees of the retail store's parent company knew about and may have promoted these transactions.

Other Reported Activities

Filers submitted a small number of SAR-Cs alleging casino patrons displayed unusual behavior, or violated the casinos' internal policies. Examples include:

- Customers who persistently inquired about the CTR-C reporting requirements, and if their buy-ins and/or cash-outs had already reached the reporting threshold. In answering their inquiries, most casino employees reportedly recited the CTR-C regulation or provided the patrons with an informational card, and refused to answer about their individual thresholds.
- A high-stakes player who frequently wired funds via depository institutions to the personal front money account of another high-stakes customer. The casino believed that if the two individuals had an outside business relationship, they should settle it directly with each other rather than through a casino deposit account.
- A customer who recorded all his wins on his player rating account and all his losses on two other patrons' player rating accounts in an effort not to look like a problem gambler in order to obtain a large-sum investment loan.
- A casino employee brought in a large sum of her own money in old bills to exchange for new ones claiming she would receive a better exchange rate when traveling to Southeast Asia because new bills do not have any markings.
- A few casino employees assisted customers by failing to record their multiple currency transactions on multiple transactions logs.
- Although not a violation of casinos' internal policies, SAR-Cs reported casino employees that bought prepaid cell phones for a recruiter. One casino employee reportedly made \$800 in one weekend buying and reselling prepaid phones. The reporting casino indicated awareness that criminals engaged in such activity.

Analysis of Inquiries from Casinos and Card Clubs Regarding Suspicious Activity Reporting (SAR) Requirements

By FinCEN's Office of Outreach Resources

FinCEN operates a Regulatory Helpline that provides assistance for financial institutions seeking clarification of their BSA and certain USA PATRIOT Act requirements and obligations.¹⁴ This article analyzes the 60 inquiries regarding suspicious activity reporting requirements that the Regulatory Helpline received from representatives of casinos and card clubs during 2008 and 2009.¹⁵ The article also highlights helpful FinCEN guidance for the most frequently asked inquiries: what constitutes suspicious activity and when it is permissible to disclose SAR-C information.

Key Volume and Geographic Trends



14. Financial institutions can contact FinCEN's Regulatory Helpline at 800-949-2732.

15. All information provided in this publication has been aggregated to ensure the confidentiality of individual inquiries. For simplicity, we will use the term "casinos" and "card clubs" within this article to mean representatives from those organizations. Determination of entity type is primarily based upon caller self-identification.

From January 1, 2008, through December 31, 2009, the Regulatory Helpline received 60 inquiries from casinos and card clubs regarding their SAR-C obligations. Inquiries strictly related to SAR-C issues totaled 16 percent of all BSA questions received from casinos and card clubs during that period. Inquiries came from 22 States, the District of Columbia, and Puerto Rico, with the majority from California or Nevada (10 each) and Michigan or Missouri (6 each).

2008 inquiries

During 2008, the Regulatory Helpline received 25 SAR-C related inquiries from casinos—there were no card club inquiries. The number of inquiries was fairly steady throughout the year until increasing in September; volume peaked in December with approximately one-third of all inquiries occurring during that month. The increase in September and December may have been related to the August publication of FinCEN's *Guidance on [Recognizing Suspicious Activity - Red Flags for Casinos and Card Clubs](#)* (FIN-2008-G007). For the entire year, the vast majority (64 percent) of the inquiries were from three States: Nevada (seven), Michigan (six), and Mississippi (three).¹⁶

2009 inquiries

By contrast, the number of SAR-C related inquiries from casinos (34) and card clubs (1) in 2009 steadily increased through May and then declined sharply through August. There was no apparent reason for this trend. In July, FinCEN published its *Advisory on Structuring by Casino Patrons and Personnel* (FIN-2009-A003). The number of inquiries rose again in September and October, with approximately one-third of all inquiries occurring in those months. Also in October, FinCEN published additional guidance for the industry, *Frequently Asked Questions – Casino Recordkeeping, Reporting, and Compliance Program Requirements* (FIN-2009-G004). During the year, nearly half of the inquiries came from California (eight), Missouri (five), and Oklahoma (four).

Key Issues and Themes

The most common issues and themes that representatives of casinos and card clubs raised with the Regulatory Helpline involved guidance on what constitutes suspicious activity, how to complete a SAR-C, and when it is appropriate to share or

16. Geographic location is based upon the area code of the caller.

disclose a SAR and related supporting information. There appears to have been no significant difference in the topics of inquiry based upon type or geographic location of the institution.

Identification of Key Issues and Themes January 1, 2008 - December 31, 2009			
Number of inquiries - 2008		Number of inquiries - 2009	
SAR sharing and disclosure	9	Definitions and other guidance	14
Other subpoena and disclosure questions	6	General guidance	7
Sharing SARs with regulators	2	FinCEN guidance	3
Attempt to obtain SARs in a civil case	1	Proposed rulemaking	3
		Regulation	1
Definitions and other guidance	7		
FinCEN guidance	3	Guidance on whether to file a SAR	12
Regulation	2	Guidance on attempted activity	7
Definitions	1	Monetary Thresholds	4
General guidance	1	Whether to file a SAR	1
Assistance with SAR form	4	SAR Sharing and Disclosure	4
SAR item instructions	3	Sharing SARs with law enforcement	3
Form corrections	1	Other subpoena and disclosure questions	1
Guidance on whether to file a SAR	3	Verification of SAR filing	3
Monetary thresholds	3	Verification of filing	2
Verification of filing	2	Obtaining copies of a SAR	1
Verification of filing	2	Assistance with SAR Form	2
		SAR item instructions	1
2008 Total	25	Form corrections	1
		2009 Total	35
Total Inquiries for January 1, 2008 – December 31, 2009			60

To address these common inquiries from casino and card club representatives, FinCEN has published a number of guidance pieces, frequently asked questions, targeted advisories, and other useful documents:

Useful Guidance on SAR-C Filing Requirements and Form Assistance

Casinos and card clubs frequently seek clarification regarding when they have an obligation to file a SAR-C and how to complete the report. Because determining whether to file a SAR-C is an inherently risk-based decision based upon specific facts and circumstances, casinos and card clubs should have policies, procedures and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating such activity. To assist with this obligation, FinCEN has published information on these topics in previous *SAR Activity Reviews*. The October 2007 and 2009 *SAR Activity Reviews*, for example, provide general guidance for all covered institutions on what constitutes suspicious activity and how to complete a SAR filing properly.¹⁷

FinCEN also has issued guidance specifically for casinos and card clubs on completing the SAR-C form. Casinos should use the December 2003 publication, [*Suspicious Activity Reporting Guidance for Casinos*](#), as a supplement to the SAR form instructions. Casinos also should consult the November 2007 [*Frequently Asked Questions - Casino Recordkeeping, Reporting, and Compliance Program Requirements*](#) (FIN-2007-G005), which addresses how comprehensive a casino's procedures must be for detecting suspicious activity (question 14); how a casino can complete a SAR-C for "unknown" subjects (question 15); and, what type of information law enforcement has found valuable from SAR-C filings (question 17). Casinos and card clubs also should refer to the August 2008 guidance (FIN-2008-G007) highlighted earlier in this article for practical examples or "red flags" from industry examiners and law enforcement that may indicate the presence of money laundering, terrorist financing, or related financial crimes. The July 2009 advisory (FIN-2009-A003) warns against potential structuring activities that law enforcement has identified as having occurred at certain casinos.

SAR-C Sharing and Disclosure: Useful Guidance

Casinos and card clubs frequently seek the guidance of FinCEN's Regulatory Helpline when law enforcement and regulatory authorities request SAR information and supporting documentation; an institution also may receive a request for SAR information to support a civil case or from someone other than an appropriate law enforcement or supervisory authority. FinCEN provided a compilation of related guidance on this topic for all covered institutions in the October 2009 *SAR Activity*

17. See [*The SAR Activity Reviews Issue 12*](#) (October 2007), Section 4 and [*Issue 16*](#) (October 2009), Section 4.

Review.¹⁸ The previously discussed October 2009 guidance (FIN-2009-G004) also includes information on what the SAR non-disclosure provision means for a casino or card club (question 16) and what type of information may be disclosed in response to a subpoena, summons, or other process issued in civil litigation (question 18).

How Examiners Use BSA Data to Scope and Plan Casino Examinations

Internal Revenue Service

IRS conducts BSA compliance examinations of casinos and other businesses that have been designated as financial institutions under the BSA and its implementing regulations but that do not have a Federal regulator. The purpose of a BSA casino examination is to determine the adequacy of a casino's BSA compliance.

Casinos have numerous BSA recordkeeping and anti-money laundering (AML) program requirements, along with the requirement to file BSA reports that have maximum utility to law enforcement. BSA casino examinations include reviewing and analyzing these filed BSA reports as well as identifying any failures to file BSA reports through a risk based audit plan. A critical process for the IRS in the scoping and planning phase (pre-audit) of a BSA casino examination involves an extensive review and analysis of all BSA reports filed by and on the casino. A thorough review and analysis of the BSA reports filed by the casino is used to determine their adequacy as well as identify trends.

Adequacy of Reports

A BSA report is deemed adequate if it is timely, complete, and accurate. The determination of the timeliness of CTR-Cs is easily and routinely accomplished in the pre-audit phase of an examination. The determination of the timeliness of SAR-Cs, however, may need to be completed after a review of internal casino

18. See [The SAR Activity Review Issue 16](#) (October 2009), Section 2. There, it was noted that FinCEN issued guidance in June 2007 entitled [Suspicious Activity Report Supporting Documentation](#) (FIN-2007-G003); institutions also were referred to [The SAR Activity Review Issue 7](#) (August 2004), Section 4.

documentation. The determination of the completeness and accuracy of BSA reports is accomplished in the pre-audit phase and as warranted in the transaction testing phase of an examination. The IRS Detroit Enterprise Computing Center sends correspondence to paper document filers for possible incomplete data in certain critical CTR-C fields. Other than correspondence for SSN mismatches, this correspondence is initiated solely based on the information contained in a single CTR-C. A correction made through correspondence does not correct all identical errors made by the filing entity, only the error on the specific document that generated the correspondence. Conversely, a BSA examiner will evaluate a casino's filed CTR-Cs and SAR-Cs collectively and compare them with other data. For example, an examiner may compare casino licensing information with Secretary of State corporate information to verify the accuracy of a filer's legal and trade names used in the BSA reports.

CTR-Cs and SAR-Cs are routinely downloaded by filer Employer Identification Number (EIN) and variations of the filer name to ensure that a complete population of all filed BSA reports is reviewed for the examination period. Use of macros and download programs provides an examiner with effective and efficient analysis tools. An examiner can easily sort the downloaded BSA reports by any field to find anomalies such as missing information or variances in filer data. The analysis for anomalies or inaccurate data on filed reports includes, but is not limited to, identifying the following:

- Any missing critical fields of the person(s) involved in the transaction if the requirement for the data was known or should have been known at the time of the transaction.
- Inconsistent or incorrect filer data (EIN, legal name, trade name, address, and institution type).
- A post office box number is used for the casino address.
- A post office box number is used for a person involved in a CTR-C transaction (a post office box number is acceptable if the casino, when presented with a post office box number, uses due diligence to determine that a person has no permanent address).
- Failure to adhere to the instructions for completing the report such as failing to use an "XX" as instructed in certain fields if the data is not applicable in paper filings.

- Failure to adhere to amended report instructions. Note: the instructions to amend a CTR-C are different than those for amending a SAR-C. Amended paper CTR-Cs must have a copy of the original attached, the amended box checked, the entire filer section completed, and only the fields changed for Part I and Part II. An amended SAR-C must be completed in its entirety, must include in the narrative a description of what fields were changed, and the amended box must be checked.
- Data inconsistent with transaction data or other internal casino data.
- Insufficient SAR-C narratives (narratives should sufficiently describe the who, what, when, where, and why).
- Supportive documentation attached to a filed SAR-C. The SAR-C instructions explicitly state that supportive documentation must be retained but not attached to filed SAR-Cs.
- SSN mismatch correspondence issued by the IRS Enterprise Computing Center on paper filed CTR-Cs.

Trends in Reports

An examiner will review and analyze a casino's broad historical trends as well as detailed transaction trends of filed BSA reports for the current time period. Although there are no targeted volumes of CTR-Cs or SAR-Cs, overall filing history trends and data trends in the reports are compared to other data such as gross annual gaming revenue, types of gaming offered, and types of transactions offered. This comparison combined with a review of the AML program is then used by the examiner to facilitate the scope and planning of the examination. For example, a CTR-C analysis may indicate that a casino may not be aggregating different types of transactions when each type individually is \$10,000 or less. The following are additional examples of possible trends that may prompt the examiner to adjust the examination plan to determine the cause:

- Most or all SAR-Cs filed describe completed transactions instead of attempted transactions or vice versa.
- Most or all SAR-Cs are filed on transactions occurring in the cage instead of the gaming floor or vice versa.

- Most or all SAR-Cs are filed on transactions in a single gaming floor area instead of in all gaming areas. For example, gaming floor SAR-Cs have only been initiated from table game and slot transactions but never from race and sports book transactions; and
- Most or all SAR-Cs filed are from real time observations instead of a review of records or vice versa. The examiner will determine if a real time suspicious activity observation could have been detected from a review of records and if not then why and vice versa.

Other BSA Report Analysis

To ensure adequate BSA compliance, the examiner will also review other BSA reports filed by the casino such as CMIRs,¹⁹ FBARs,²⁰ or Form 8300s.²¹ If these types of reports are not filed and other sources indicate that there may be a requirement to file, the examiner will adjust the examination scope to include additional audit steps to verify compliance. The examiner will also review and evaluate any BSA report filed on the casino by other casinos, money services businesses, banks, or other industries subject to BSA requirements. If warranted, the examiner will then adjust the examination scope.

The SAR Activity Review - By the Numbers as a Resource

By FinCEN's Office of Regulatory Analysis

How Financial Institutions can benefit from By the Numbers

The SAR Activity Review - By the Numbers (BTN) is another valuable resource with data from which financial institutions can benefit on both a micro and macro level. BTN summarizes Suspicious Activity Report (SAR) data relative to several reported categories that, in some cases, are common across financial sectors and, at other times, are unique to a specific industry.

19. Reports of International Transportation of Currency or Monetary Instruments

20. Reports of Foreign Bank and Financial Accounts

21. Report of Cash Payments Over \$10,000 Received in a Trade or Business

Financial Crimes Enforcement Network

The SAR data is divided into four sections which encompass multiple exhibits for each industry.

	Depository Institutions (Form TD F 90-22.47)	Money Services Businesses (FinCEN Form 109)	Casinos and Card Clubs (FinCEN Form 102)	Securities & Futures Industries (FinCEN Form 101)
Filings by Year & Month	✓	✓	✓	✓
Filings by States & Territories	✓	✓	✓	✓
Number of Filings Ranked by States & Territories in Descending Order	✓	✓	✓	✓
Number of Filings by Characterization or Type of Suspicious Activity in Descending Order	✓	✓	✓	✓
Number of Filings by Characterization or Type of Suspicious Activity	✓	✓	✓	✓
Filings by Primary Federal Regulator	✓			
Filings by Financial Services Involved		✓		
Filings by Type of Gaming Establishment			✓	
Filings by Instrument Type				✓
Filings by Relationship of Subject to Financial Institution	✓		✓	
Filings by Type of Reporting Institution				✓
Characterization or Type of Suspicious Activity by State & Territory by Year	✓	✓	✓	✓

Macro level analysis encompasses categories common to all industries and allows filers to broadly view the data based on: time (Filings by Year), geography (Filings by States & Territories), or rationale (Type of Suspicious Activity). Presented individually at first, these three topics are then brought together into a spreadsheet which further breaks down the reported suspicious activity by State & territory and year.

Financial Crimes Enforcement Network

BTN Issue 13 (January 2010)

Section 1 - Suspicious Activity Report Form TD F 90-22.47 for Depository Institutions

Exhibit 2: Suspicious Activity Report Filings by States & Territories

April 1, 1996 through June 30, 2009

State/Territory	1996 - 1999*	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009**	Total
Alabama	1,824	689	1,156	1,263	1,579	2,343	3,904	5,249	5,062	5,656	3,073	31,798
Alaska	423	353	287	420	487	1,022	2,153	2,038	2,028	2,585	955	12,751
American Samoa	10	10	2	8	3	29	28	56	107	174	87	514
Arizona	9,952	3,894	4,350	12,680	12,078	11,481	13,775	14,023	12,885	14,710	8,702	118,530
Arkansas	1,317	560	694	956	1,031	1,057	1,559	1,760	1,792	2,269	1,249	14,244
California	83,213	43,304	54,467	63,489	68,546	94,123	130,655	123,794	149,990	147,171	63,484	1,022,236
Colorado	5,137	2,146	3,526	6,857	3,766	5,054	7,349	7,571	6,768	7,874	3,987	60,035
Connecticut	6,616	4,873	4,445	4,231	2,385	2,870	3,499	6,733	7,313	6,986	3,428	53,379
Delaware	6,254	3,670	4,360	6,660	6,595	9,119	14,614	17,111	29,854	39,367	27,037	164,641
District of Columbia	968	467	594	909	826	1,206	1,428	1,537	1,888	2,845	1,705	14,373
Federated States of Micronesia	7	3	1	3	3	1	0	2	7	5	0	32
Florida	26,193	9,918	12,434	17,389	15,650	17,319	25,135	33,067	36,923	49,868	28,309	272,205
Georgia	6,345	3,141	4,112	5,634	5,696	6,885	9,069	11,836	11,653	15,738	8,881	88,990
Guam	246	73	90	131	78	130	234	349	710	684	397	3,122
Hawaii	2,063	731	982	1,189	1,455	1,593	2,012	3,970	7,112	8,104	3,633	32,844
Idaho	586	402	401	414	432	638	1,060	1,130	943	1,043	555	7,604
Illinois	11,394	4,790	5,727	10,146	12,707	13,910	17,137	20,118	21,800	23,265	11,751	152,745
Indiana	3,527	1,349	1,638	2,526	2,695	3,616	5,480	5,650	6,363	7,429	3,357	43,630
Iowa	1,411	493	838	960	905	1,511	1,856	1,813	2,046	2,206	1,040	15,079
Kansas	1,498	520	838	1,506	2,016	2,270	2,592	2,801	2,682	3,022	1,742	21,487
Kentucky	1,898	853	1,334	1,859	1,910	2,622	3,284	3,065	3,171	3,536	1,795	25,327
Louisiana	2,712	1,943	2,312	2,725	2,596	3,730	4,844	5,627	4,973	4,896	2,731	39,089
Maine	733	241	325	429	718	752	1,032	1,914	2,353	2,083	905	11,485
Marshall Islands	2	0	1	3	0	0	1	1	3	4	0	15
Maryland	4,371	2,069	2,249	3,662	3,137	4,613	5,470	6,232	7,445	8,442	4,994	52,684
Massachusetts	6,683	2,747	3,220	5,274	5,541	7,559	8,471	11,287	13,413	14,959	6,177	85,331
Michigan	7,726	3,765	4,880	6,049	7,687	10,788	12,004	12,309	12,379	13,028	10,123	100,738
Minnesota	8,078	2,893	3,379	4,461	4,064	6,102	7,272	6,657	6,404	8,279	3,116	60,705
Mississippi	940	521	693	729	889	1,399	2,182	2,712	3,110	3,496	1,774	18,445
Missouri	4,045	1,590	2,472	2,791	2,873	3,425	5,335	7,181	9,752	13,147	7,122	59,733
Montana	434	220	284	249	319	452	758	691	805	693	367	5,272
Nebraska	1,151	615	835	3,560	3,417	1,919	1,744	1,474	1,582	1,753	968	19,018
Nevada	6,495	3,074	3,221	3,584	4,451	6,159	8,722	8,705	7,562	11,155	5,724	68,852
New Hampshire	1,873	448	1,018	944	793	1,060	1,400	1,582	1,525	1,620	770	13,033
New Jersey	8,294	4,197	5,694	7,873	10,209	18,714	16,086	17,355	17,903	20,059	11,028	137,412
New Mexico	1,077	403	502	869	856	1,041	1,727	1,485	1,492	1,570	757	11,779
New York	47,308	19,138	23,737	30,729	30,225	39,045	58,168	58,019	65,806	68,054	31,759	471,988
North Carolina	7,126	2,978	3,238	3,589	3,562	5,876	11,366	13,897	15,903	17,752	11,129	96,416
North Dakota	597	224	224	256	201	288	378	371	387	377	203	3,506
Northern Mariana Islands	71	57	41	68	30	51	73	109	232	283	157	1,172
Ohio	7,386	3,319	4,536	6,173	8,561	10,850	16,650	19,498	18,841	19,432	10,962	126,208
Oklahoma	2,113	813	897	1,233	1,397	1,746	2,576	2,779	3,380	3,878	2,188	23,000
Oregon	4,744	2,471	2,813	2,254	2,192	2,392	3,711	3,519	3,734	4,051	1,903	33,784
Overseas	96	22	20	14	23	68	128	209	737	473	177	1,967
Palau	0	0	3	1	3	2	10	10	28	46	12	115
Pennsylvania	10,202	3,535	4,498	6,713	7,549	11,474	14,896	16,321	17,977	19,554	10,624	123,343
Puerto Rico	1,524	1,063	1,237	1,836	2,423	3,922	3,944	4,599	6,158	7,043	4,622	38,371
Rhode Island	1,256	495	530	1,204	1,393	1,368	1,618	2,134	2,229	3,229	1,473	16,929
South Carolina	2,105	733	963	1,323	1,307	1,962	2,616	3,657	4,327	4,617	2,619	26,229
South Dakota	1,988	267	478	3,546	3,891	4,522	5,547	5,965	8,593	13,803	5,839	54,439
Tennessee	3,289	1,555	2,036	2,162	2,706	4,280	7,464	9,184	9,378	12,317	6,428	60,799
Texas	23,095	10,119	13,426	17,203	17,611	23,231	32,561	36,097	38,036	43,310	22,952	277,641
U.S. Virgin Islands	41	32	58	68	78	94	108	370	647	452	178	2,126
Unknown/Blank	428	19	34	250	491	793	2,540	2,220	4,747	7,192	5,899	24,613
Utah	3,716	2,219	2,673	3,425	4,441	6,277	11,888	13,046	15,470	17,938	3,778	84,871
Vermont	272	69	98	132	176	229	488	673	646	621	323	3,727
Virginia	5,513	2,001	3,014	3,536	4,771	6,053	8,109	11,836	15,711	18,138	11,814	90,496
Washington	7,844	3,362	3,989	3,561	4,103	5,575	7,706	7,309	7,232	9,406	4,581	64,668
West Virginia	590	182	173	298	463	865	1,169	1,307	1,305	1,402	784	8,538
Wisconsin	2,376	1,006	1,260	1,666	2,021	3,787	4,660	4,699	5,115	6,256	3,575	36,421
Wyoming	167	67	201	151	332	409	410	367	759	595	316	3,774

*Filing years 1996 - 1999 represent an aggregate total for this period.

**Issue 13 numerical data is for the years 1996 through the first half of 2009. The full 2009 numbers will appear in Issue 14.

Note: Suspicious Activity Report statistical data is continuously updated as additional reports are filed and processed. For this reason, there may be minor discrepancies between the statistical figures contained in various portions of this report or in previous reports.

Financial Crimes Enforcement Network

Micro level analysis of SAR data includes information unique to each of the reporting industries: Filings by Primary Federal Regulator (depository institutions), Filings by Financial Services Involved (money services businesses), Filings by Type of Gaming Establishment (casinos and card clubs), and Filings by Instrument Type and by Type of Institution (securities & futures industries).

BTN Issue 13 (January 2010)

Section 2 - FinCEN Form 109 : Suspicious Activity Report by Money Services Business (SAR-MSB)

Exhibit 6: SAR-MSB Filings by Financial Services Involved*

October 1, 2002 through June 30, 2009

Financial Services Involved	2002	2003	2004	2005	2006	2007	2008	2009**
Money Order	549	70,024	90,954	116,196	172,470	233,880	170,657	75,985
Traveler's Check	49	1,149	1,419	1,183	2,192	3,537	3,655	1,931
Money Transfer	4,769	129,655	183,728	232,717	289,722	308,302	316,310	174,089
Other	179	5,118	15,931	28,970	26,445	28,596	24,065	12,430
Unknown/Blank	223	4,337	5,016	5,526	7,318	9,819	12,968	4,987
Currency Exchange***	-	-	-	-	-	384	2,181	584

*Some SAR-MSBs may list multiple services.

**Issue 13 numerical data is for the years 2002 through the first half of 2009. The full 2009 numbers will appear in Issue 14.

***FinCEN Form 109 (formerly TD F 90-22.56), which replaced the original SAR-MSB form, became effective on March 31, 2007. Form 109 added "box e"(Currency Exchange) to Part II, field 19.

BTN Issue 13 (January 2010)

Section 3 - FinCEN Form 102: Suspicious Activity Report by Casinos and Card Clubs (SAR-C)

Exhibit 6: SAR-C Filings by Type of Gaming Establishment

August 1, 1996 through June 30, 2009

Type of Gaming Establishment	1996 - 1999*	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009**
State Licensed Casino	572	309	1,215	1,621	4,393	4,696	4,680	4,969	6,726	7,616	3,933
Tribal Licensed Casino	250	115	114	120	539	935	1,254	2,140	2,992	3,108	1,519
Card Club	6	1	1	9	19	27	46	39	41	216	103
Other	3	0	0	0	1	1	5	6	15	3	3
Unspecified/Blank	309	45	48	84	165	121	101	182	188	238	112

*Filing years 1996 - 1999 represent an aggregate total for this period.

**Issue 13 numerical data is for the years 1996 through the first half of 2009. The full 2009 numbers will appear in Issue 14.

Another component of the micro view includes data about the relationship (e.g., Customer, Employee, Officer, etc.) that a subject has with the filing institution. Below are examples from BTN that show relationships described in depository institution SARs and casino and/or card club SAR-C filings.

Financial Crimes Enforcement Network

BTN Issue 13 (January 2010)

Section 1 - Suspicious Activity Report Form TD F 90-22.47 for Depository Institutions

Exhibit 7: Relationship of Suspect to Financial Institution

April 1, 1996 through June 30, 2009

Relationship	1996 - 1999*	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009**
Accountant	195	63	82	159	198	315	532	582	547	398	174
Agent	780	503	523	1,078	661	956	1,138	745	947	1,212	565
Appraiser	170	122	372	476	881	2,172	2,531	3,827	4,262	5,909	3,142
Attorney	120	45	47	67	74	104	191	179	217	367	151
Borrower	13,941	5,100	6,151	6,809	8,866	14,410	19,988	32,414	53,727	68,034	29,463
Broker	1,313	965	1,512	1,702	2,450	4,516	7,453	12,497	16,688	20,332	6,510
Customer	221,621	110,463	142,780	198,177	198,952	273,868	373,439	395,043	452,146	509,756	259,897
Director	500	154	190	210	209	209	268	236	229	309	189
Employee	31,043	10,851	11,693	11,445	12,337	13,165	14,629	16,032	16,454	17,928	8,034
Officer	2,054	565	694	763	730	791	838	997	1,185	1,130	354
Shareholder	1,808	562	740	689	758	1,320	1,329	1,848	2,127	2,002	694
Other	51,994	21,822	28,256	36,157	41,016	52,586	77,175	93,790	107,882	124,399	64,115
None Indicated	65,986	25,582	25,969	33,996	40,193	41,046	55,193	55,884	54,863	60,717	39,367

*Filing years 1996 - 1999 represent an aggregate for this period.

**Issue 13 numerical data is for the years 1996 through the first half of 2009. The full 2009 numbers will appear in Issue 14.

BTN Issue 13 (January 2010)

Section 3 - FinCEN Form 102: Suspicious Activity Report by Casinos & Card Clubs (SAR-C)

Exhibit 7: SAR-C Filings by Relationship of Suspect to Financial Institution

August 1, 1996 through June 30, 2009

Relationship	1996 - 1999*	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009**
Customer	861	440	1,340	1,798	4,540	5,183	5,446	6,954	9,506	10,551	5,407
Agent	11	4	10	7	45	43	110	88	119	170	57
Junket/Tour Operator	2	0	1	2	1	3	1	0	0	3	1
Employee	11	1	9	7	14	21	9	23	38	59	25
Check Cashing Operator	1	0	0	0	1	0	1	0	1	0	0
Supplier	0	0	0	1	0	0	1	0	1	2	0
Concessionaire	75	3	4	5	8	3	2	5	4	3	0
Other	0	0	0	0	36	35	27	46	76	95	26
Unknown/Blank	185	22	21	20	529	518	604	275	338	444	249

*Filing years 1996 - 1999 represent an aggregate total for this period.

**Issue 13 numerical data is for the years 1996 through the first half of 2009. The full 2009 numbers will appear in Issue 14.

As all the information presented within BTN has been collected since the time each industry was required to report suspicious activity, readers may track filed data by individual year or over the course of multiple years, thus getting a historical or recent perspective of the reporting rates for each category as mentioned above.

Financial Crimes Enforcement Network

For example, a financial institution interested in studying the prevalence of a particular type of suspicious activity, may refer to BTN to review the trends for the activity as reported in SARs. Since BTN is published bi-annually, an institution can also see if there was an increase or decrease in the rate of reporting between 6-month intervals.²² The table below shows yearly filing data for the types of suspicious activity reported in SAR-Cs through 2009.

BTN Issue 13 (January 2010)
Section 3 - FinCEN Form 102: Suspicious Activity Report by Casinos & Card Clubs (SAR-C)
Exhibit 5: Number of SAR-C Filings by Type of Suspicious Activity*
 August 1, 1996 through June 30, 2009

Type of Suspicious Activity	1996 - 1999**	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009***
Bribery/Gratuity	11	1	4	1	10	14	15	36	32	28	21
Check Fraud (Includes Counterfeit)	16	9	18	18	112	161	114	260	344	336	173
Credit/Debit Card Fraud (Includes Counterfeit)	10	3	9	2	53	87	17	65	68	84	44
Embezzlement/Theft	4	1	10	3	23	22	21	45	36	66	45
False or Conflicting ID(s)	0	0	0	0	246	441	425	717	1,196	1,183	555
Large Currency Exchange(s)	44	28	56	45	271	317	322	357	381	464	225
Minimal Gaming with Large Transactions	156	89	333	436	824	1,096	1,149	1,277	2,197	2,655	1,331
Misuse of Position	4	0	8	7	7	11	9	15	26	43	14
Money Laundering	137	36	83	79	217	295	324	277	373	431	246
No Apparent Business or Lawful Purpose	31	19	61	158	343	326	405	411	555	732	431
Other	388	158	428	714	1,513	1,423	1,639	2,310	2,468	2,463	1,284
Structuring	344	186	558	636	2,296	2,469	2,568	2,661	3,533	4,588	2,234
Terrorist Financing	0	0	0	0	12	1	1	4	12	3	2
Unknown/Blank	151	28	63	35	53	79	70	85	90	114	50
Unusual Use of Counter Checks or Markers	0	0	0	0	221	43	129	269	401	450	225
Unusual Use of Negotiable Instruments (Checks)	8	0	18	7	79	72	94	202	306	304	184
Unusual Use of Wire Transfers	12	4	9	11	54	74	50	45	78	83	47
Use of Multiple Credit or Deposit Accounts	1	1	3	7	4	18	10	11	15	8	14

*Some SAR-Cs may list multiple suspicious activities.

**Filing years 1996 - 1999 represent an aggregate total for this period.

***Issue 13 numerical data is for the years 1996 through the first half of 2009. The full 2009 numbers will appear in Issue 14.

Besides assessing filing rates on a nationwide scale, filers may also use BTN to track suspicious activity data state-by-state, perhaps in states where the filer has branch locations or conducts business. Financial institutions can also use the BTN data to augment their own studies, either by inputting figures manually into Excel tables, or downloading them directly into their own system(s) for further manipulation and analysis.

22. Some anomalies, such as noticeable spikes or dips, are generally highlighted in BTN's Introduction section. Readers should consider how the entire body of numbers can be used to improve their efforts to mitigate risks and report information useful to law enforcement.

Financial Crimes Enforcement Network

BTN Issue 13 (January 2010)
Section 3 - FinCEN Form 102: Suspicious Activity Report by Casinos & Card Clubs (SAR-C)
Exhibit 8¹: SAR-C Filings by Type of Suspicious Activity by State & Territory by Year*
 August 1, 1996 through June 30, 2009

¹This Exhibit is partial - a full list of states is available in BTN 13.

*This Exhibit does not include SAR-Cs where the State is Unknown/Blank (or) where the Type of Suspicious Activity is Unknown/Blank (or) Both

**Filing years 1996 - 1999 represent an aggregate total for this period.

***Issue 13 numerical data is for the years 1996 through the first half of 2009. The full 2009 numbers will appear in Issue 14.

Note: Suspicious Activity Report statistical data is continuously updated as additional reports are filed and processed. For this reason, there may be minor discrepancies between the statistical figures contained in the various portions of this report or in previous reports.

State/Territory	Type of Suspicious Activity																
	Bribery/Gratuity	Check Fraud	Credit/Debit Card Fraud	Embezzlement/Theft	Large Currency Exchange(s)	Minimal Gaming with Large Transactions	Misuse of Position	Money Laundering	No Apparent Business or Lawful Purpose	Structuring	Unusual Use of Negotiable Instruments	Use of Multiple Credit or Deposit Accounts	Unusual Use of Wire Transfers	Unusual Use of Counter Checks or Markers	False or Conflicting Ids	Terrorist Financing	Other
Nevada																	
1996 - 1999**	9	8	2	2	11	38	2	17	21	123	3	0	3	0	0	0	113
2000	0	8	1	0	5	12	0	8	8	52	0	0	0	0	0	0	34
2001	1	7	1	1	1	28	2	16	17	35	1	0	3	0	0	0	45
2002	0	11	1	3	6	24	4	12	15	57	1	1	3	0	0	0	47
2003	4	15	5	3	20	119	2	23	60	515	9	0	27	7	35	1	372
2004	2	12	12	2	17	151	0	34	70	373	15	1	30	4	48	1	164
2005	5	10	3	2	10	135	0	63	88	436	24	1	20	7	43	0	102
2006	4	118	7	11	9	105	2	32	66	465	47	3	22	6	67	0	79
2007	9	142	10	17	41	323	12	73	189	1,147	142	10	68	16	162	2	200
2008	9	142	27	38	41	484	16	97	328	1,319	137	3	50	37	274	0	202
2009***	1	109	16	19	17	215	7	68	153	643	43	4	19	59	146	0	109
Total	44	582	85	98	178	1,634	47	443	1,015	5,165	422	23	245	136	775	4	1,467

In addition to displaying SAR data in Excel, even-numbered editions of BTN illustrate the aggregated figures of selected information in graph, chart, and map formats, thus offering readers other perspectives of the same data and enabling them to see new or unrecognized patterns of suspicious activity.

Following are explanations of how some of the data in BTN is calculated. This information is provided for institutions that want to use SAR counts as provided in BTN (in whole or in part), and combine them with their own data.

- **Filings by Year:** The numeric tabulation of SARs and the time frame(s) they relate to are both computed using a Document Control Number (DCN). The DCN is a unique number assigned to all SARs by the IRS's Enterprise Computing Center (ECC).²⁵ The DCN specifies the calendar date of receipt at IRS, as well as the type of form and the manner in which it was submitted, either paper or electronically. DCNs also contain a series of sequential numbers that correspond to each individual SAR.
- **Filings by States & Territories:** Geographic representations generally reflect where the suspicious activity occurred²⁶ and are derived from data entered in the transaction location field. In some instances, SARs may name multiple places where the activity took place and, depending on the form, these locations are also listed among the Filings by States & Territories.
- **Type of Suspicious Activity:** SARs submitted by financial institutions often indicate more than one type of suspicious activity. All activities, whether reported as the only suspicious activity on a SAR or listed in combination with other activities, are individually counted and then aggregated for that type of suspicious activity.

For example, an institution files two SARs, one citing Check Kiting as the characterization of suspicious activity and the other listing Check Fraud and Check Kiting. These would be tabulated as two instances of Check Kiting and one instance of Check Fraud (not one instance of Check Kiting and one instance of Check Fraud and Check Kiting).

Note: Since May 2, 2006, certain segments of the insurance industry have been required to report suspicious activity and instructed to use FinCEN Form 101 (Suspicious Activity Report by the Securities and Futures Industries²⁷). Until numeric tabulations based on a dedicated SAR form for insurance companies

25. The IRS data center responsible for maintaining Bank Secrecy Act (BSA) data which includes, amongst other forms, SARs.

26. This may also include the foreign office or branch of an institution which, while domestically located, has reported the location as where the activity occurred.

27. This factor should be taken into account when reviewing and/or utilizing SAR data concerning the securities and futures industries beginning with the May 2006 effective date.

are made available through BTN, those interested in reviewing figures related to insurance industry filings should refer to the following publications: *Insurance Industry Suspicious Activity Reporting: An Assessment of Suspicious Activity Report Filings* (April 2008)²⁸ and *Insurance Industry Suspicious Activity Reporting - An Assessment of the Second Year of Suspicious Activity Report Filings* (January 2010).²⁹

In addition to providing information that may be useful to financial institutions, *By the Numbers* may prove useful to other segments of its wide-ranging readership. These include, among others, Federal, State and local law enforcement; regulatory agencies; the intelligence community; private industry; and academia.

Readers are encouraged to contact FinCEN's Regulatory Helpline at 1-800-949-2732 should they require guidance in navigating the various sections of BTN, accessible through FinCEN's web-site at www.fincen.gov under Reports & Publications.

28. See http://www.fincen.gov/news_room/rp/reports/pdf/Insurance_Industry_SAR.pdf.

29. See http://www.fincen.gov/news_room/rp/files/Insurance_update_pub.pdf.

Section 3 - Law Enforcement Cases

This section of *The SAR Activity Review* affords law enforcement agencies the opportunity to summarize investigations where BSA information played an important role in the successful investigation and prosecution of criminal activity. This issue contains new case examples from Federal and local law enforcement agencies. Additional law enforcement cases can be found on the FinCEN website under the link to Investigations Assisted by BSA Data. This site is updated periodically with new cases of interest, which are listed by the type of form used in the investigation, type of financial institution involved, and type of violation committed.

Contributing editors: Shawn Braszo, Vanessa Morales, James Emery, Jack Cunniff, Len Senia.

In this edition of the SAR Activity Review, we focus on cases where defendants either pled guilty or were convicted at trial on BSA-related violations. We present these examples because FinCEN has seen an increasing number of cases where defendants have been charged with structuring or failing to comply with reporting requirements. Prosecutors are increasingly charging defendants with these violations, particularly when the underlying criminal activity is difficult to prove in court. For example, proving structuring, where an individual made deposits of \$9,900 for several days in a row, can be shown with a simple bank statement. Structuring, with the intent of evading CTR filing is in itself a Federal violation, with a criminal penalty of up to 5 years imprisonment and a possible fine of up to \$250,000. If the structuring involves more than \$100,000 in a 12-month period or is performed while violating another Federal law, the penalty is increased to imprisonment not to exceed 10 years and/or a fine of \$500,000.³⁰

We start with a case where the defendant was laundering money from an illegal escort service through a casino. Then we highlight a case where the defendant was laundering funds derived from criminal activity, but Federal prosecutors had few options but to charge the defendant with structuring. In the third case, a defendant, who had joint access to a bank account with her mother, withdrew all the funds without her mother's knowledge. Prosecutors used the structuring statutes to

30. See 31 USC § 5324(d).

charge the defendant and were able to recover some of the funds. The fourth case is highly unusual because the defendant clearly structured funds, but without any nexus to criminal activity.

The next two cases highlight instances where individuals failed to comply with BSA reporting requirements. A jewelry store owner did not report the large currency payments he received from drug dealers, and then in turn proceeded to structure those proceeds into the bank. In the second case, a doctor failed to report a foreign bank account and then, when the account was closed, structured shipments of currency into the United States.

Finally, we look at an innovative use of CTRs to identify tax violators. CTRs are still vitally important to law enforcement, and this example illustrates that dutiful compliance with reporting requirements enables investigators to identify criminal behavior.

Casino Money Laundering Prosecution

Escort Service Operates at and Launders Money through Casino

Case summary. Two individuals, who frequented a tribal casino, operated a local escort service and conducted a prostitution business at the casino. Defendant A was often in the company of young females who would meet and then leave with males from the casino for short periods. Upon return to the casino, the females would again meet up with Defendant A, the director of the escort service. Surveillance images from the casino confirmed that Defendant A was not only associating with the young females, but spent a great deal of time on a cellular phone – behavior consistent with the operation of an escort service. The cash that the prostitutes received from these illegal acts was given to the escort service and the service paid the prostitutes directly from these funds. The escort service was used as a front for organized prostitution. Besides managing the escort service while at the casino, Defendant A used the casino to launder the remaining proceeds from these criminal activities.

Case details. The escort service generated so much money that Defendant A became one of the top bettors at the casino, primarily playing electronic slot machines. Slot player tracking records from the casino reveal that during a 4-year period Defendant A individually inserted over \$3,000,000 in cash into electronic gaming devices' bill acceptors/validators. Defendant A recycled funds through the machines by downloading credits onto a casino players card, or from some machines by the issuance of slot ticket vouchers, which all were redeemed at the cashier's cage. Defendant A's cash-out totals resulted in over a 94% return of funds and a total loss of only \$200,000. Defendant A also obtained slot vouchers from the machines that could be redeemed at the cashier's cage – which then could be used as payments for the prostitutes.

Defendant A pled guilty to 2nd degree promotion of prostitution and money laundering, and was sentenced to 24 months in State prison and forfeited a house. Defendant B, who frequently drove the escorts to and from locations to engage in acts of prostitution and who collected money from the escorts for the director of the escort service, was charged with 2nd degree promotion of prostitution, and was sentenced to 134 days in State prison

BSA Cases in the News

Paralegal Found Guilty at Trial on Structuring Charges

Case summary. A lawyer and his paralegal assistant devised a scheme to defraud multiple credit card companies through a bankruptcy filing as a means to fund a real estate purchase. The pair structured the fraudulent proceeds through multiple banks to disguise the funds' origins. Although the lawyer eventually pled guilty and cooperated with authorities, the paralegal insisted on going to trial; she was found guilty. A Federal judge sentenced the paralegal to between one and two years in prison.

Case details. In 2007, a Federal jury found the paralegal guilty of charges including conspiracy and structuring transactions to avoid the filing of CTRs. Her co-conspirator had pled guilty earlier and testified against her. The two orchestrated a credit card bust-out scheme in and out of several bank accounts. The paralegal structured the funds from the scheme and eventually purchased real estate property with the proceeds of the crime.

All transactions related to the crime occurred from early 2002 through early 2003. During a seven-month period in 2002, the lawyer obtained approximately \$270,000 in credit card loans from at least 20 different credit card issuers. He deposited approximately \$260,000 of credit-card loan proceeds into five accounts he held in his name at four different banks.

As a first step in the conspiracy, the lawyer withdrew approximately \$200,000 in cash, all proceeds of his credit card loans, from these bank accounts. He structured the cash withdrawals in amounts of less than \$10,000 to avoid the filing of CTRs. He then handed most of this cash to the paralegal so that she could deposit it, in a structured manner, into accounts she opened in her name at two banks.

As charged in the indictment, between April and September 2002, the paralegal deposited approximately \$160,000 in cash she had received from the lawyer into the accounts. She subsequently withdrew approximately \$180,000 in cash, in a structured manner, from her accounts at the banks. The lawyer structured all those cash withdrawals in amounts of less than \$10,000.

During early 2003, the two defendants deposited approximately \$200,000, in a structured manner, into three accounts held in the paralegal's name at branches of several banks.

In early 2003, the paralegal wrote a check, drawn on her bank account and funded by money traceable to the credit card fraud scheme, as a down payment to purchase a residence.

In early 2003, the paralegal withdrew approximately \$180,000 from her account – again, all proceeds of the structured currency transactions and of the credit card fraud scheme – to pay the balance for the property.

The lawyer testified that, as part of his and the paralegal's scheme, he obtained money from credit card loans, and transferred the cash to her in a manner that would avoid the issuance of CTRs. The paralegal used the cash to buy a house in her name, thereby concealing she had bought the house with money obtained from the lawyer's credit cards. The two planned to transfer his other assets to her and then file for bankruptcy to wipe out the credit card debts.

At trial, the paralegal admitted making the cash deposits alleged in one count of the indictment, the cash withdrawals alleged in another count, and the second set of cash deposits alleged in a third count. She also admitted that she was aware that banks had to report to the government cash transactions involving more than \$10,000. She further admitted that she structured the cash transactions, albeit at the lawyer's alleged behest, for the purpose of avoiding the CTR filings.

Following a trial, a federal jury found the paralegal guilty of all five counts against her: one count of conspiring to structure financial transactions and four counts of structuring financial transactions for the purpose of avoiding the banks' issuance of CTRs.

In addition to the prison term, the presiding judge ordered her to pay restitution to the credit card companies. The judge also ordered that the residence that the two conspirators had bought in her name with the proceeds of their conspiracy be forfeited to the government. At sentencing, the government advised the Court that it intended to turn over the restituted funds obtained from the sale of the forfeited house to the victims of the offense.

Structuring Charges Help Elderly Victim Recover Stolen Funds

Case summary. A woman was sentenced in 2010 after pleading guilty to a structuring charge resulting from the theft of funds from her elderly mother. Although the defendant received a relatively light sentence, the assistant U.S. attorney prosecuting the case noted that structuring was the only criminal charge the government could bring to help retrieve the money.

Case details: In 2009, the defendant admitted in a plea agreement that the United States could prove at trial that during a two-month period in 2008, she knowingly structured financial transactions, totaling approximately \$170,000, with her mother's bank for the purpose of evading currency transaction reporting requirements of Section 5313(a) of Title 31, United States Code, and regulations promulgated there under, Title 31, Code of Federal Regulations, Section 103.22. Bank records show that within that timeframe, the daughter made approximately 20 withdrawals of \$10,000 or less.

In court documents, investigators point out that during a period of more than one year in 2007 and 2008, the daughter resided at the home of her elderly mother, and they had a joint bank account. In 2008, the daughter approached a bank employee and asked how much money she could withdraw at one time from the bank account before the bank notified the government. The bank employee did not give her the information and the daughter left the bank, but a few days later began the structured withdrawals.

While the daughter was making the cash withdrawals from the joint account, bank employees made several failed efforts to contact her mother about the transactions. When individuals attempted to visit the mother, her daughter advised them that her mother was unavailable. The mother did not enter the bank during the time of her daughter's withdrawals, but called the bank because she discovered her daughter was withdrawing her money from the bank. Her daughter subsequently entered the bank and employees questioned her about her mother being upset with her for withdrawing the money. She told the bank employees to mind their own business and withdrew approximately \$20,000, which was the amount remaining in the account. She also said that she was moving to the Pacific Northwest.

The mother filed a police report for the theft of the money as well as some jewelry. She told investigators that her daughter was a long-time alcoholic and had moved in with her with no money or possessions. Investigators identified more than \$20,000 in an account that the daughter held at a financial institution in the Pacific Northwest. They were able to seize the money and return it to her mother. All told, investigators were able to retrieve nearly \$100,000 and return it to the mother.

Judge Rules Defendant Guilty of Structuring; No Connection to Criminal Activity Alleged

Case summary. In a key decision, a defendant went to trial after pleading not guilty to two counts of structuring. Notably, in this case, prosecutors did not bring money laundering charges against the defendant because there was no indication that the structured currency resulted from any illegal activity. However, the case underscores that structuring is a crime, that prosecutors will file charges on those who attempt to evade reporting requirements, and that a guilty conviction is possible even without a direct link to any other criminal activity.

Case details. In 2009, a Federal judge found the defendant guilty of structuring financial transactions with a domestic financial institution for the purpose of causing the financial institution to fail to file a CTR required by Title 31 U.S.C. § 5313(a). The defendant was found not guilty of an additional charge of structuring.

According to the indictment, the defendant owned and operated a limousine service business located on the East Coast. During a five-month period in 2007, the defendant deposited and caused to be deposited approximately \$140,000 in cash into two accounts at a local bank. One account was in his name while the other was in the name of his business.

During the time-period cited in the indictment, the defendant made approximately 15 cash deposits at local branches. All but two of the transactions were for amounts ranging from \$9,000 to \$9,900, and none of the transactions were for \$10,000 or more. In one transaction in the indictment (and for which he was ultimately convicted) the defendant handed a teller two stacks of currency, each for \$10,000 and requested deposits into both his personal and business accounts. When the teller began to prepare a CTR, the defendant withdrew \$100 from each stack, and eventually deposited only \$9,900.

The defendant's administrative assistant told investigators that he frequently gave her money to deposit that came from his closed office. She thought this was unusual because the business did not generate the type of currency that was reflected in the large deposits.

In court documents, prosecutors originally charged the defendant with two counts of structuring transactions to evade reporting requirements, in violation of 31 U.S.C. § 5324(a) (3) and (d). Prosecutors were able to prove these charges by demonstrating that the defendant had knowledge of the reporting requirements and, structured transactions by breaking down a single sum of currency exceeding \$10,000 into smaller sums, with the purpose of evading currency reporting requirements of § 5313(a).

Jewelry Store Owner Fails to Report Large Cash Transaction, Structures Proceeds from Drug Trafficking.

Case summary. A jewelry store owner who was previously convicted of laundering funds for drug dealers was caught again accepting currency from drug traffickers in exchange for jewelry. In a sting operation, the defendant accepted approximately \$30,000 in cash from an undercover IRS agent in exchange for jewelry. The owner believed that the money he was accepting was from drug trafficking activities and tried to conceal the transaction by failing to file a Form 8300.³¹ Moreover, the defendant structured the transactions into a financial institution to disguise the funds' origins.

Case details. In 2009, the defendant pled guilty to conspiracy to launder drug proceeds. A U.S. district judge sentenced the defendant to over three years in prison, followed by 5 years of supervised release.

According to the defendant's plea agreement, he owned and operated a jewelry business. From at least 1982 until 2006, he knowingly accepted over \$300,000 in cash from drug traffickers in exchange for jewelry. According to court documents, the defendant intentionally concealed the nature of those transactions by failing to file IRS Form 8300 and by structuring certain transactions to make them appear legitimate.

For example, in 2006, as part of an investigation of the jewelry business by the IRS, the defendant accepted over \$10,000 in cash from an undercover IRS agent in exchange for jewelry. Later in 2006, the defendant accepted over \$20,000 from the same agent in exchange for jewelry. The defendant was led to believe that the agent was a drug dealer and that the money he was accepting was derived from the agent's drug trafficking. The defendant knowingly failed to file the required FinCEN Form 8300 to document the transactions.

This is the second time the defendant has been convicted on money laundering charges. In 1990, he stood trial for the same offenses and was convicted. Both prosecutions were the results of sting operations.

31. Report of Cash Payments Over \$10,000 Received in a Trade or Business

Doctor Pleads Guilty to Charges Related to Failure to Comply with BSA Reporting Requirements for Overseas Accounts

Case summary. In 2010, a United States Attorney announced that a doctor pled guilty to conspiracy to impede the United States and to making a false statement. He was facing a maximum sentence of ten years in prison and a maximum fine of \$500,000.

Case details. According to court documents, in 1997, the doctor inherited an undeclared bank account at a Switzerland branch of one of the world's largest international banks. The account was held in the name of a phony Liechtenstein trust. In 1999, the doctor met with an attorney who managed the account in Switzerland. The foreign attorney instructed the doctor to keep the account "hush," to avoid keeping any records relating to the account, and to send coded letters if he wished to meet with the attorney. Further, the attorney advised the doctor that if he transported or mailed less than \$10,000 in U.S. currency back to the United States, he would not have to declare the funds to the U.S. government upon re-entry to the United States.

Prosecutors alleged that in 2009, the doctor was informed that the international bank was closing his undeclared Swiss account and that he had until the end of the year to travel to Switzerland to withdraw all funds. He made multiple trips to Zurich in 2009 and met with his attorney at his office and a Swiss banker at the private wealth office of the international bank. The attorney and the Swiss banker refused to wire the money to the United States, as it would leave a trail for U.S. law enforcement. Instead, they provided him with approximately \$240,000 in U.S. currency. The doctor received most of the currency in individually wrapped bundles of sequentially numbered, new \$100 bills.

According to court documents, with the assistance of the attorney, the doctor mailed multiple packages containing over \$200,000 in U.S. currency from Switzerland to the United States to himself and another person.

In his plea, the doctor admitted that, upon his return to the United States, he falsely informed a U.S. Customs Inspector that he had traveled to Switzerland to purchase diamonds. Further, he falsely stated to a U.S. Customs Inspector that he had not recently mailed any U.S. currency from Switzerland into the United States. However, the plea agreement also noted that Customs and Border Protection officers seized a package containing approximately \$9,000 addressed to the defendant's residence.

Prosecutors alleged that, for the years 1997 through 2008, the doctor made and subscribed false U.S. Individual Income Tax Returns, Forms 1040, that failed to report on the Schedules B attached to the returns that he had an interest in a financial account in a foreign country. Additionally, the doctor failed to report the income he earned on his undeclared Swiss account on his tax returns.

From 1997 through 2008, the doctor failed to file with FinCEN a required Report of Foreign Bank and Financial Accounts on Form TD F 90-22.1 (FBAR) reporting his interest in his undeclared Swiss account.

As part of his plea agreement, the doctor agreed to forfeit to the government over \$200,000 in U.S. currency that law enforcement officials seized from packages that the doctor mailed from Switzerland to his residence in the United States.

United States citizens and residents have an obligation to report to the IRS on the Schedule B of a U.S. Individual Income Tax Return, Form 1040, whether they had a financial interest in, or signature authority over, a financial account in a foreign country in a particular year by checking "Yes" or "No" in the appropriate box and identifying the country where the account was maintained. United States citizens and residents also have an obligation to report all income earned from foreign bank accounts on the tax return.

United States citizens and residents who have a financial interest in, or signature authority over, a financial account in a foreign country with an aggregate value of more than \$10,000 at any time during a particular year are required to file an FBAR with FinCEN. The FBAR for the applicable year is due by June 30 of the following year.

In addition, individuals who physically transport, mail or ship, or cause to be physically transported, mailed, shipped or received, currency, traveler's checks, and certain other monetary instruments in an aggregate amount exceeding \$10,000 into the United States are required to file a FinCEN Form 105, Report of International Transportation of Currency or Monetary Instruments (CMIR), with the Bureau of Customs and Border Protection.

United States law prohibits individuals from structuring mailings of U.S. currency into the United States in amounts less than \$10,000 if the purpose of the structuring was to evade the requirement to file a CMIR.

Proactive Currency Transaction Report Reviews Lead to Tax Cheats

Case summary. In a proactive use of CTRs, the financial intelligence director with the Manhattan district attorney's office has identified hundreds of businesses that are using check cashers rather than banks as a means of evading Federal, State, and local taxes. The businesses have created, in effect, an underground economy where payments are made in cash. The district attorney has prosecuted the first of potentially hundreds of violators.

Case details. In 2009, the Manhattan, New York, district attorney announced that a defendant pleaded guilty to two counts of evading New York State and City corporate and personal income taxes. The counts are both felonies and occurred over two years.

The investigation leading to the plea revealed that the defendant operated a cash business by negotiating client checks through check cashing establishments. By paying suppliers, subcontractors, and workers with that cash, the defendant was able to conceal the true amount of the business's gross receipts and therefore underreport its profits.

Prosecutors charged the defendant with underreporting over \$1.3 million of the gross receipts on his 2005 New York City general corporation tax return, thereby underreporting his tax liability to the New York City Department of Finance. The defendant also failed to file his 2005, 2006, and 2007 personal income tax returns, and thereby failed to report earnings approaching \$300,000. The defendant did not pay any personal income tax to the New York State Department of Taxation and Finance for the period charged.

The defendant accepted a plea where he could face incarceration in a State facility if he does not comply with all terms and conditions of the plea agreement, which includes the repayment of over \$100,000 in personal income and corporate taxes, accrued interest and applicable penalties, prior to sentence. He will be required to pay the maximum criminal fine of \$100,000 and perform community service. He also will be required to submit tax filings for tax year 2009 that will account for an additional \$2.8 million of unreported gross receipts generated in that period. Each felony he is charged with is punishable by a maximum of 4 years in prison.

The district attorney said, "This case illustrates the continued existence of the underground economy. According to the New York State Banking Department, in 2008 the commercial checking industry negotiated checks totaling almost \$3 billion. All but one commercial check casher was located in New York City."

“By availing themselves of the services of check cashers, business persons conceal a substantial portion, and sometimes all, of the gross receipts of their businesses, and thereby evade several types of City and State taxes, including corporate, payroll and personal income taxes. This is not an isolated case. The investigation has disclosed hundreds of businesses that have engaged in similar conduct. The extent of the tax evasion is of staggering proportions. ”

The case began when an official with the district attorney’s office searched for CTRs filed by commercial check cashers operating in Manhattan. The number of records was substantial and the analyst saw that many of the subjects/owners were named in multiple CTRs. After downloading the CTRs, the official sorted the data and noticed patterns of activity specific to construction contractors. The BSA data revealed that the CTRs filed by check cashers described transactions by individual businesses totaling hundreds of thousands to millions of dollars per year.

The subsequent investigation uncovered that the defendant and his business had not filed tax returns during the past few years. In addition, this business is only one of over 150 that have conducted the same or similar activity reflected on CTRs. The proactive search uncovered businesses that cashed more than \$500 million in checks during the past 4 years.

Section 4 - Issues & Guidance

This section of *The SAR Activity Review* discusses current issues raised with regard to the preparation and filing of SARs and to provide meaningful guidance to filers. It reflects the collective positions of the government agencies that require organizations to file SARs.

Suggested Best Practices - Casino or Card Club Risk-Based Compliance Indicators

By FinCEN's Office of Regulatory Policy

This article describes factors that a casino or card club may need to consider in applying a risk-based approach to the development and implementation of a BSA compliance program. The BSA requires casinos and card clubs to develop and implement compliance programs tailored to business activities and customer risk profiles (e.g., type of products and services offered, the locations served, and the nature of their customers). Please note that the business/customer risk factors described below will not apply equally to all casinos and card clubs, and even when these factors are present, there may be different risk outcomes for different casinos and card clubs. A casino or card club may not be required to address each of the factors described below; also a casino or card club should not construe the risk indicators below as exhaustive and the only ones required to be addressed.

I. General Business Risk Indicators

There are many risk indicators or factors that a casino or card club may need to consider when developing and implementing an effective BSA compliance program to combat money laundering and terrorist financing. Risk factors may differ depending on the business activities of a specific gambling establishment, or its products and services, as well as State, tribal or local gambling regulations that affect the gaming operation. Also, a casino or card club may need to consider the risk management principles that it applies in its operational areas when assessing and managing its BSA risk profile.

A casino or card club may need to consider, as appropriate, the following factors when developing and implementing risk-based policies, procedures, internal controls and systems to comply with the BSA:

- Gross annual gaming revenue (GAGR) of the business as well as GAGR by type of gambling offered (*e.g.*, table games, card games, slot machines, video lottery terminals, sports book betting, pari-mutuel wagering on horse or dog races).
- Overall physical layout of gambling establishment (*e.g.*, square footage and gambling floor layout).
- Governmental wagering limitations or other legal constraints on betting or the types of games offered.
- Types of gambling offered (*e.g.*, table games, card games, slot machines, video lottery terminals, sports book betting, pari-mutuel wagering on horse or dog races).
- Types of specific games offered (*e.g.*, roulette, baccarat/mini-baccarat, or craps, which allow a pair of bettors to cover between them both sides of an even bet).
- Number of table games, card games, slot machines/video lottery terminals offered.
- Number of table games, slot machines or video lottery terminals with high dollar maximum bet limits.
- Number and location of cages and slot redemption booths.
- Number of cage windows and race/sports book windows.
- Number of slot kiosks for ticket redemptions and maximum dollar thresholds.
- Types of financial services offered at the cage (*e.g.*, deposit accounts, credit/marker accounts, account access cards, check cashing accounts, currency exchange services), any limitations on financial services, and other types of payment methods accepted (*e.g.*, credit cards, debit instruments, wire transfers).
- Types of negotiable instruments accepted for cashing, credit, deposit, and purchase of gaming instruments (*e.g.*, business checks, cashier's checks, foreign drafts, domestic or international money orders, official bank checks, personal checks, promissory notes, third-party checks, domestic or foreign traveler's checks).

- Business and personal check cashing dollar limits.
- Whether customers can wire funds domestically or internationally through a domestic depository institution for deposit or payment of markers into their personal casino accounts.
- Whether a third-party contractor provides check cashing or money transmitting for customers on the premises.
- Whether a third-party contractor provides race and sports book wagering within a casino, and the extent to which a casino conducts such customer transactions on behalf of a third-party contractor.
- Types of financial transactions that a casino “host” can conduct on behalf of customers.
- Whether customers are allowed to conduct transactions through chip runners and the types of transactions that can be conducted.
- Whether the casino or card club is located in a High Intensity Financial Crime Area (“HIFCA”).³²
- Whether the casino or card club is located in a High Intensity Drug Trafficking Area (“HIDTA”).³³
- Whether the casino or card club is located in a town or city center, or in a more remote location.
- Whether the casino or card club is located near a U.S. land border crossing.
- Proximity of the casino or card club to any interstate freeways which allow customers quick ingress and egress to the gambling operation.
- Whether the casino or card club is owned by a State or tribal government, privately owned, a combination of State and private entities, or is a publicly traded company.

32. Locations designated as HIFCAs enable a concentration of law enforcement efforts at the Federal, State, and local governmental levels. For a listing, see www.fincen.gov/hifcaregions.html.

33. Locations designated as HIDTAs are provided additional Federal government resources to help eliminate or reduce drug trafficking and its destructive consequences. For a listing, see the Office of National Drug Control Policy’s website at www.whitehousedrugpolicy.gov.

- Whether a casino is owned by a corporation that operates other casinos in the same state or other states, as well as other countries.
- Number of employees, experience levels, and turnover rate of key personnel and frontline employees.
- Number of surveillance employees and ratio of employees to surveillance cameras.
- Number of fiduciary accounts that are opened annually (*e.g.*, deposit accounts, credit/marker accounts, check cashing).
- Number of marketing accounts that are opened annually (*e.g.*, player rating and slot club).
- Geographic marketing areas, such as international, regional, and local marketing areas, as well as relative concentration in these markets.
- Business clientele model and profile (*e.g.*, a large number of customers who gamble relatively small amounts of money, a large number of customers who gamble relatively large amounts of money, a small number of customers who gamble relatively small amounts of money, a small number of customers who gamble relatively large amounts of money, or some combination of these).
- Customer base (number of accountholders versus estimated number of non-accountholders, organized casino tours/junkets, estimated number of local customers versus estimated number of travelers or tourists).

II. Customer Risk Indicators

Although any type of customer activity is potentially vulnerable to money laundering or terrorist financing, certain customers may pose specific risks. In assessing customer risk, casinos and card clubs may need to consider other variables, such as services sought, products used, and geographical locations. For example, a casino or card club may need to consider the following:

- Particular aspects of operations (*i.e.*, products, services, games, and accounts or account activities) that can be used by customers to facilitate money laundering and terrorist financing.
- Non-resident aliens and foreign nationals with deposit accounts who are citizens of countries or jurisdictions that are:

- Identified as non-cooperative by the Financial Action Task Force (FATF)³⁴.
 - Identified as Jurisdictions of Concern or Jurisdictions of Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR).³⁵
 - Designated as jurisdictions of primary money laundering concern or subject to special measures through regulations issued by FinCEN pursuant to Section 311 of the U.S.A. PATRIOT Act.³⁶ or
 - Sanctioned by the Office of Foreign Assets Control (OFAC), including those with state sponsored terrorism.³⁷
- Customers with significant levels of gambling (*e.g.*, in amounts of \$3,000 - \$10,000 inclusive) that are non-accountholders and for which identification is not known and is unavailable.
 - Customers that pose higher risks based on type of account, account activity, types of products and services used, geographic locality, or player rating, *etc.*.
 - Customers that engage in a relatively high level of spending.
 - Customers engaged in high value gambling that are inconsistent with a casino or card club's information about levels or sources of assets or incomes, or inconsistent with information about occupations in casino credit/marker account records (*e.g.*, credit/marker applications) or other records.
 - Customers using deposit accounts for non-gambling purposes.
 - Customers observed borrowing money from non-conventional sources, including other customers.
 - Customers conducting transfers of significant or unusual amounts of funds through depository institutions.

34. FATF is an inter-governmental body whose purpose is the development and promotion of policies, at both the national and international levels, to combat money laundering and terrorist financing. See www.fatf-gafi.org.

35. See www.state.gov/p/inl/rls/nrcrpt.

36. See www.fincen.gov/reg_section311.html.

37. See www.treasury.gov/offices/enforcement/ofac/programs/.

- Customers using domestic or international money orders in amounts just below the threshold for recordkeeping requirements, traveler's checks denominated in foreign currency, domestic wire transfers in amounts just below the threshold for recordkeeping requirements, debit cards, and prepaid access (stored value) cards either in significant numbers or with significant total monetary value.
- Customers conducting large transactions with minimal casino play.
- Regular customers with unusual spending pattern changes (*e.g.*, dramatic or rapid increases in the size and frequency of transactions).
- Customers listed on a so-called "barred patron list" and their known associates.
- Customer player rating and slot club accounts with P.O. Boxes only instead of permanent street addresses.
- Periodic review of FinCEN Form 102, SAR-Cs filed that are based on direct observation of customer activity and review of customer records.
- Dollar value of intercompany transfers of funds from customers' accounts for front money deposit or marker redemption conducted between casinos in the United States and their affiliated casinos located in other countries.

Once a casino or card club has identified the specific risk factors unique to its operation, it should conduct a more detailed analysis of its level of vulnerability. The level and sophistication of the analysis may depend on the comprehensiveness of a casino's or card club's risk assessment process or the risk factors that apply. Also, the results may differ according to its business risk model and governmental gambling regulations. By understanding its risk profile, a casino or card club can apply appropriate risk management processes to its BSA compliance program to identify and mitigate its operational risk.

In conclusion, an effective BSA compliance program must reflect potential money laundering and terrorist financing risks arising from a casino's or card club's products, services, customer base, and geographical location. Casinos or card clubs may need to update their risk indicators to reflect changes in operational risk profiles (*e.g.*, revised products and services, new products and services, changes with regard to opening and closing accounts or closer monitoring of accounts, new categories of accounts, or changes resulting from acquisitions or mergers). It is a sound practice for a casino or card club to periodically review its risk indicators or factors to assure sufficiency and effectiveness.

For questions about this guidance, please contact FinCEN's Regulatory Helpline at (800) 949-2732.

* * * * *

For additional guidance, see *Frequently Asked Questions – Casino Recordkeeping, Reporting and Compliance Program Requirements*, FIN-2007-G005 (November 14, 2007) and FIN-2009-G004 (September 30, 2009). Other reference material includes *Suspicious Activity Report Filings Within the Casino and Card Club Industries, The SAR Activity Review, Trends, Tips and Issues, Issue 8* (April 2005) and [FinCEN SAR Bulletin, Issue 2: Suspicious Activities Reported by Casinos](#) (August 2000).

Casino or Card Club Compliance Assessment *By FinCEN Office of Regulatory Policy*

This article describes factors that a casino or card club may need to consider in assessing the effectiveness of its BSA compliance program. The BSA requires casinos and card clubs to develop and implement compliance programs tailored to their business activities and risk profiles. A casino or card club may not need to address each of the factors described in this document. Also, a casino or card club should not construe the factors below as exhaustive and the only ones required to be addressed.

I. Elements of a BSA Compliance Program

A casino or card club is required to develop and implement a BSA compliance program that adequately addresses the risks posed by its products, services, customer base, and geographical location for the potential of money laundering and terrorist financing. At a minimum, each BSA compliance program³⁸ must provide for:

- A system of internal controls to assure ongoing compliance with the BSA.
- Internal or external independent testing for compliance with a scope and frequency commensurate with the risks of money laundering and terrorist financing posed by the products and services provided.

38. See 31 CFR § 103.64(a). Compliance with this requirement satisfies the obligation under Section 352 of the USA PATRIOT Act to implement an anti-money laundering (AML) program. See 31 CFR § 103.120(d).

- Training of casino personnel, including training in the identification of unusual or suspicious transactions.
- An individual or individuals to assure day-to-day compliance with the BSA.
- Procedures for using all available information to determine and verify, when required, the name, address, social security or taxpayer identification number, and other identifying information for a person.
- Procedures for using all available information to determine the occurrence of any transactions or patterns of transactions required to be reported as suspicious.
- Procedures for using all available information to determine whether a record required under the BSA must be made and retained.
- For casinos and card clubs with automated data processing systems, use of the programs to aid in assuring compliance.

II. Criteria for Assessing a BSA Compliance Program

A casino or card club may need to consider the following criteria, among others, when assessing its BSA compliance program:

- Management awareness and commitment to compliance.
- Comprehensiveness of policies, procedures, and internal controls and whether policies, procedures, and internal controls need updating.
- Level and frequency of training and whether training is appropriate for the business and compliance functions performed by personnel (*e.g.*, front-line employees).
- Compliance officer's authority, responsibilities, and extent of control and effectiveness, as well as the expertise of the compliance staff.
- Effectiveness of a compliance committee (if established).
- Adequacy of internal or external audit reports in confirming whether the independent review:
 - Evaluated the comprehensiveness of the BSA compliance program and was conducted by an individual knowledgeable of the BSA's requirements.

- Provided a fair and unbiased appraisal of the BSA compliance program, including BSA-related policies, procedures, and internal controls, as well as other requirements such as reporting and record retention.
- Determined whether the casino or card club is operating in compliance with the requirements of the BSA and the casino or card club's own policies, procedures and internal controls.
- Included testing of internal controls and transactional systems and procedures to identify problems and weaknesses and, if necessary, recommend to management appropriate corrective actions.
- Any BSA compliance deficiencies identified by audit reports and effectiveness of any subsequent corrective actions taken.
- Extent of usage of appropriate automated systems and programs to support its compliance program.
- Adequacy of account opening and documentation policies, procedures and processes.
- Adequacy of policies, procedures and processes for the types of financial services offered or types of negotiable instruments accepted.
- Adequacy of procedures and processes for filing currency transaction reports.
- Adequacy of procedures and processes for detecting suspicious transactions or patterns of suspicious transactions and filing suspicious activity reports.
- Whether there are areas of the operation which require special compliance considerations (*e.g.*, creation of specific types of records, availability of records, records retention).
- Whether supervision of employees is adequate.

III. Basis for Revising a BSA Compliance Program

Based on its assessment, a casino or card club should consider the following in determining whether to revise its BSA compliance program:

- Results of independent testing, including internal or external reviews or audits.
- Results of examinations by the Internal Revenue Service or other governmental authorities.

- Significant changes in cage or floor operations.
- Significant changes in the types of financial services offered or types of negotiable instruments accepted.
- Implementation of automated systems and programs that affect compliance.
- Amendments to BSA regulations.
- Amendments to BSA reporting forms.
- New BSA guidance or advisories including “frequently asked questions.”
- *SAR Activity Reviews – Trends, Tips & Issues*, with articles on casinos, card clubs or gambling as well as Suspicious Activity Report (SAR) bulletins.
- The extent to which CTR-Cs filed during specified time frames were:
 - filed late.
 - included P.O. Boxes for customers’ addressees.
 - omitted critical information items.
- The extent to which the casino or card club received correspondence indicating that CTR-Cs were filed that included errors or omissions that prevented processing, or indicating the existence of reporting errors or omissions, such as:
 - no street address.
 - incorrect social security numbers.
 - no date of birth.
- The extent to which SAR-Cs, had:
 - no subject information.
 - no characterization of suspicious activity.
 - inadequate narratives.

Deficiencies could result in BSA civil money penalties or other enforcement actions. Also, a casino or card club may need to consider corrective action, as appropriate. Deficiencies that may warrant taking corrective action include, but are not limited to the following:

- Failure to implement a compliance program.
- A significant breakdown in internal controls or lack of adherence to policy, procedures and controls to assure compliance with the BSA.
- Inadequate testing, training, or other failures in an essential element of a BSA compliance program.
- Compliance program continues to be deficient or violations continue to occur after the institution becomes aware of problems.
- Failure to file SAR-Cs when warranted:
 - Failure to investigate potential suspicious activity.
 - Failure to document reason for deciding not to file a SAR-C for activity initially identified as potentially suspicious.
 - Failure to include all relevant information in a SAR-C.
- Failure to file CTR-Cs.
- Filing of CTR-Cs that lack key information (*i.e.*, customer name; address; SSN or other government identification number;³⁹ identification credential with issuer and number; amount of currency; or date of transaction).
- Failure to create or retain required records or to provide all the information required by those records.
- Management participation in BSA violations.
- Assisting customers in structuring transactions to evade the reporting or recordkeeping requirements.

In conclusion, an effective BSA compliance program should reflect a casino or card club's products, services, customer base, and geographical location. It is a sound practice for a casino or card club to periodically re-assess its BSA compliance program to assure sufficiency and effectiveness.

39. When a SSN is not entered on a CTR-C in the case of a foreign national, a foreign country code as well as passport number or non-resident alien registration number must be recorded. *See* FinCEN Form 102, Instructions, Item 12, for country code.

Financial Crimes Enforcement Network

For questions about this guidance, please contact FinCEN's Regulatory Helpline at (800) 949-2732.

* * * * *

For additional guidance, see *Frequently Asked Questions – Casino Recordkeeping, Reporting and Compliance Program Requirements*, FIN-2007-G005 (November 14, 2007) and FIN-2009-G004 (September 30, 2009), and *Recognizing Suspicious Activity - Red Flags for Casinos and Card Clubs*, FIN-2008-G007 (August 1, 2008). Other reference material includes *Structuring by Casino Patrons and Personnel*, FIN-2009-A003, (July 1, 2009). See also *In the matter of the Tonkawa Tribe of Oklahoma and Edward E. Street* - FinCEN No. 2006-1 (March 24, 2006).

Section 5 - Industry Forum

In each issue of *The SAR Activity Review*, representatives from the financial services industry offer insights into some aspect of compliance management or fraud prevention that present their view of how they implement the BSA within their institutions. The *Industry Forum* section provides an opportunity for the industry to share its views. The information provided may not represent the official position of the U.S. Government.

Anti-Money Laundering (AML) Programs and Nevada’s Casino Industry - Training and the Methods Used for Detection of Money Laundering and Fraud

By: Thomas A. Peterman, Senior Vice President and General Counsel for MGM Grand Hotel & Casino, representing the American Gaming Association on the Bank Secrecy Act Advisory Group; and Peggy Zimmer Jacobs, Executive Director—Casino Controller and Compliance Officer for MGM Grand Hotel & Casino

Casinos as Financial Institutions

Luxurious hotel suites, gourmet restaurants, night clubs, top-name entertainment in showrooms and arenas, swimming pools, gaming tables and slot machines. The first thought that comes to mind might be a well earned vacation at a Las Vegas resort. The first thought would not be — a financial institution. Nonetheless, since 1993, casinos have been included within the BSA through 31 CFR 103’s (“Title 31”) definition of “financial institutions.”⁴⁰ This inclusion is despite the fact that casinos do not make loans⁴¹ (but may extend credit) – unlike other

40. See 31 CFR § 103.11(n).

41. See *Nguyen v State*, 116 Nev. 1171, 14 P. 2d 515 (2000).

financial institutions, such as banks, credit unions and brokerage companies, which also offer interest bearing accounts or issue cashier's checks, money orders or traveler's checks.

Perhaps the biggest distinction between casinos and other financial institutions is that a casino customer can conduct a transaction in virtual anonymity. Assuming that reporting thresholds are not met, bets can be made, chips can be cashed and no form of identification is needed. On the contrary, when an individual opens an account or applies for a loan, banks and other financial institutions require substantial personal and business information. When the loaning of money is involved, an extensive credit check is conducted and often collateral is required before the loan transaction can be finalized. Unless a casino customer is requesting marker signing privileges without placing comparable funds on deposit, it is not in a casino's business model to obtain detailed personal information or be concerned with a customer's occupation or business. Even when a person applies for "credit" at a casino, neither government regulation, nor the casino's normal business practice requires it to use the same in-depth inquiry used by other financial institutions to determine a person's ability to repay the debt established. However, what casinos and other financial institutions do have in common is that they conduct incoming and outgoing wire transactions, cash checks (including traveler's checks), exchange foreign currency and, most notably, deal in transactions that involve large amounts of cash. Because of these similarities to other financial institutions, casinos provide an opportunity for lawbreakers to launder money obtained illegally, assist in the evasion of tax liability and can unwittingly be used for terrorist financing.

AML Training and Nevada's Casino Industry

State licensed casinos generally became subject to BSA provisions in 1985. However, because Nevada's stringent regulatory system "substantially [met] the reporting and recordkeeping requirements" of the BSA, including the requirement to file suspicious activity reports with the Nevada Gaming Control Board, it was exempted from compliance with Title 31 by the Department of the Treasury. The exemption relating to suspicious activity reports was repealed in March 2003 and on July 1, 2007, Nevada casinos, with annual gross gaming revenue of \$1,000,000 or greater, became obligated to comply with Title 31's currency transaction reporting and recordkeeping requirements.

While recordkeeping and the filing of currency transaction reports are important aspects of Title 31's regulatory scheme, suspicious activity reports provide law enforcement agencies and the Federal government with the most effective means of detecting criminal activity and terrorist financing. With the passage of the USA PATRIOT Act in 2001, casinos and other financial institutions were required to put more focus on the actions of their customers and the methods and manner by which transactions were taking place. In that regard, FinCEN repeatedly has reminded financial institutions that the narrative portion of suspicious activity reports is instrumental in assisting law enforcement agencies in their efforts to uncover fraud, money laundering, and/or terrorist financing activity.

In December 1994, Treasury made significant amendments to its casino regulations which, among other things, required the development of a written compliance program. Thereafter, in September 2002, FinCEN issued a final rule to require casinos and card clubs to report suspicious transactions relevant to a possible violation of law or regulation, as well as an obligation to enhance casino compliance programs. The final rule became effective on March 25, 2003. See 67 F.R. 60722-60729 (Sept. 26, 2002). The amendments related to compliance programs provided for: (1) internal and/or external independent testing with the scope and frequency commensurate with the risks of money laundering and terrorist financing as well as the products and services provided; and (ii) procedures designed to detect occurrences or patterns of unusual or suspicious transactions. Internal controls and written policies and procedures may look impressive on paper, but without an effective training program, a casino is likely to fall short of its Title 31 obligations.

All employees who go through training should receive general knowledge of AML laws and the importance of detecting suspicious activity. However, it is imperative that training be specific to the job duties and responsibilities of the individual employee. All newly hired employees should receive training prior to functioning in a capacity where they may encounter a transaction governed by Title 31. AML training should thereafter be required on a regularly scheduled, periodic basis. In many cases, casinos employ a diverse group of individuals from different backgrounds, as well as, many regions of the world. Because of that, and in order to have an effective compliance program, employees need to understand the reasons why the BSA and USA PATRIOT Act were enacted and why Title 31 regulations require recordkeeping and the filing of reports. By doing so, the employees are in a better position to recognize the importance of the laws and why those laws are instrumental in our collective effort to combat criminal activity and terrorist financing. Again, emphasis should be placed on the BSA requirements to detect and report suspicious activity occurring in the casino industry.

To be effective, training should provide real world examples of the type of customer activity which is considered suspicious and which casino employees may be expected to encounter when performing their day-to-day job responsibilities. After all, suspicious activity may occur through a casino floor or cage employee's interaction with customers, or in the context of transactions over which the casino's financial department employees perform audit functions. With such training, employees will gain the knowledge necessary to report conduct by customers that should be brought to the attention of the casino's compliance officer or the casino's compliance committee.

For the above reasons, training is perhaps the most important part of any Title 31 AML compliance program, and it should cover the specific risks of the individual licensee.

The creation and implementation of, and the ongoing modification to, an AML training program are imperative if a casino is to comply with its regulatory obligations. Similarly, any meaningful system for detection and prevention of money laundering or potential terrorist financing is impossible without cooperation of the individuals working within casinos or other financial institutions. Casino employees are, for all intents and purposes, the experts in their industry. Therefore, they are in a unique position to provide law enforcement agencies and government officials with a sense of what type of transactions and/or whether activity by a customer may appear to lack a legitimate business purpose, or is not the sort of activity in which a customer may be expected to engage.

Methods Used to Detect Fraud

Fraud in the casino industry takes varying forms. Sometimes it is directly committed against the casino. For example, a customer may present a counterfeit cashier's check as a front money deposit against which to draw markers. Or a group of customers, each of whom has signature authority on the same bank account, may obtain separate marker authorization limits which exceed the total of funds in that account. Due to practices of certain banks, each person who has signature authority on an account will be reported to the casino by the bank as having access to the totality of funds in the account. When the customers have no intention of honoring the payment of the markers, the casino becomes a victim of the fraud.

More often, the casino unknowingly is used as a vehicle for individuals to perpetrate a fraud on third parties or launder funds obtained illegally. Under those circumstances a casino can use its internal records, implement varying practices and take advantage of the Internet tools available to detect and then report such suspicious activity.

Fraud and other suspicious activity can take on many forms and there isn't a net big enough to capture or detect the numerous vehicles used by individuals seeking to outsmart the government. Casinos need to rely on the eyes and ears of their staff, electronic/computer reports generated by the casino's table games and slot management systems, and a comprehensive audit review in order to effectively implement its AML program. It is simply not prudent for casinos to have only one method or a limited number of methods to detect suspicious activity of its customers. When people think of the types of activities that may be considered suspicious they immediately think of cash (currency). While it is true that structuring transactions in an effort to avoid currency reporting remains the most common type of suspicious activity report being filed, criminals are creative in their efforts to avoid detection of their illegal activity.

For example, with regard to structuring transactions, casinos need to develop reports that can analyze customer activity over a specific, yet flexible period of time. A casino must be capable of viewing the broad landscape of transactions and use its computer systems, as it is foolhardy to believe that front line staff can detect transactions just under the \$10,000 reporting threshold over different days, shifts, and throughout the physical layout of the casino.

Casinos also need to carefully review marker play. Once completed by a Nevada gaming licensee as authorized by Nevada Revised Statute 463.368, a marker is no different than a bank counter check (i.e., it contains (i) a payee; (ii) is signed by a drawer (the customer); (iii) is dated; (iv) sets forth a sum certain; and (v) is imprinted with the customer's bank account number). See Nevada Gaming Commission Regulation 6.118. Like other negotiable instruments, a completed marker can be deposited into the casino's bank account and thereafter be processed for payment through the banking system.

Marker play occurs in two forms. In one situation, a customer may deposit cash or cash equivalents (e.g., cashier's check, traveler's checks, personal check, etc.) at the casino cage. The cage cashier will place (and record) the funds into what is generally referred to as a front money deposit account. Thereafter, the customer may withdraw all or a portion of the funds deposited by requesting and signing a marker. In exchange for signing the marker(s) the customer will receive chips at a gaming table, or tokens to play a slot machine in an amount not to exceed the amount of funds placed on deposit.

The second way that markers are used is when the customer has established a marker authorization limit with the casino. In other words, the customer has not placed any cash or cash equivalents on deposit, but the casino has made the business decision to permit a customer to be given chips (or tokens or slot machine credits) with which to gamble, based upon the customer's perceived ability to repay. In order to permit customers to use markers when no front money has been deposited, the casino must adhere to internal controls required by the State. Simply stated, a casino must use internal or external information and records to establish that the customer has the financial wherewithal to repay the casino, since there is no front money deposit available to satisfy the indebtedness. Although the vast majority of marker play is legitimate, it does provide an avenue for an individual to engage in suspicious activity.

The use of marker authorization limits (i.e., issuing markers without a comparable front money deposit), coupled with a struggling economy and a criminal element, creates a "perfect storm" for suspicious transactions. Some individuals use markers to obtain chips, not for casino play, but for illegal activity and later conversion to cash. For example, situations have arisen where customers who have established a marker authorization limit obtain chips which, without the knowledge of the casino, are later loaned to third parties, at high interest rates – in other words, for illegal loan sharking purposes. For this reason, a customer's play must be evaluated for discrepancies. There likely is no legitimate reason for a customer to sign \$50,000 in markers, if their win/loss for a trip is only \$2,000. When a scenario like this occurs (large transactions with minimal play), it is the responsibility of the casino to determine where the \$48,000 in chips went. If no legitimate reason can be established, a suspicious activity report will be filed.

Another reason for taking large markers and not playing involves identity theft. A customer will set up a marker authorization limit using another person's identity, draw the entire amount down as quickly as possible, and leave the casino without satisfying the debt established. At a later date, the customer, usually with the aid of others in their group, will cash out the chips in small amounts (less than \$3,000), so as not to cause the filing of a currency transaction report or draw the attention of cashier employees. These front line employees are trained to question a customer who seeks to cash out large amounts of chips by inquiring where in the casino the customer obtained the chips to be cashed out. When a statement of outstanding balance is sent to the person whose identity has been stolen, or when the markers are deposited and later rejected by the bank, only then will the identity theft be discovered.

In addition to their own computer systems, casinos should use available third party resources in order to have a comprehensive program for detecting fraud and suspicious activity. Some of the resources available include internet search engines for general information on its customers, as well as a subscriber service that provides detailed personal information about a customer, their businesses and their associates. Casino compliance personnel also should make themselves aware of media reports that involve their customers. Law enforcement and grand jury subpoenas which are served on casinos provide compliance personnel with yet another source with which to investigate customer activity. When the casino receives a subpoena on an individual, its personnel can review casino system information to take a closer look at the types of activity these individuals have engaged in within the casino. Oftentimes, a look back at transactions which occurred months or even years before can result in the determination that the customer engaged in suspicious activity. For example, it may be found that the subject of a subpoena had gaming activity that corresponded with the time frame during which the accused was suspected of conducting a Ponzi scheme or embezzling funds from a business. If so, a suspicious activity report will be filed.

Conclusion

The key to having a meaningful system for detecting varying types of suspicious activity is to have an AML program that is fluid. A casino must be willing to periodically take a fresh look at the risks within its property and evaluate its processes to ensure that those processes are relevant. Equally important, a casino must keep its training programs current and modify those programs to assure its employees are given the tools with which to perform their BSA obligations effectively. When it comes to suspicious activity, casinos need to be one step ahead of those customers who engage in unsavory activity, and if they cannot stay ahead of them, the casino needs to detect the reportable suspicious activity on the back end.

Bank Secrecy Act Compliance Challenges in an Environment of Declining Revenue

By Joe H. Smith, Director of Audits, National Indian Gaming Commission

The philosopher Adam Smith described the capacity of putting one's self in the place of another, to experience what they feel, to understand their motives and desires: "By the imagination we place ourselves in his situation ... we enter as it were into his body and become in some measure him." Continuing, Smith described this capacity as "the source of our fellow-feeling for the misery of others." In today's economy, particularly in tribal gaming, often the person most to be pitied in the gaming enterprise is that of the general manager or other individual responsible for the gaming conducted.

In years past, when, with little effort, gross revenues were increasing year after year, operational deficiencies, or the consequence thereof, could be whitewashed over with volume. In some areas, the market was expanding at a faster rate than could be satisfied and management success depended little upon intuition or competency. Praise and bonuses flowed generously and self aggrandizing perspectives of invincibility were common. However, the gaming environment has shifted. Benefits that once represented low hanging fruit now must be earned, and the competition may be fierce.

General Managers were once viewed with admiration by casino staff due to the mystical feats of wonder they seemed to produce at will but, today, as he or she walks across the casino floor in route to the office, a smirk often runs across the face of staff as they wonder how long this one will last. It has become a job in which satisfying the expectation of the stakeholders has become a Herculean, if not an impossible, endeavor. As gross revenues have declined in recent years, management has been tasked with ensuring that operating expenses maintain parity with the volume conducted; however, debt obligations were generally negotiated when times were good. Loan terms, inclusive of high interest rates and restrictive covenants, which hardly mattered when negotiated, require operators today to juggle liquidity and margins to stay on the right side of the agreements.

To exacerbate the situation, many tribal governments have acquired an insatiable appetite for the profits of their gaming operation(s). Not unlike other government programs, entitlement programs, once established, grow beyond initial estimates and, once recipients develop a dependency, it is difficult to reduce benefits. Since gaming is typically the dominant revenue source for tribal governments, management is put into a precarious position in which failure to meet expectations is virtually assured. Net income is declining, lenders are expecting loan covenants to continue to be satisfied, and tribal government officials are demanding ever increasing cash distributions. The drawing and quartering of casino management represents a spectacle being played out in many gaming operations, both commercial and tribal. So, what has management done to try to satisfy these competing interests?

Essentially, management has had to shorten its strategic planning cycle so that satisfaction of operational objectives is measured in months as opposed to years. Performance benchmarks are identified for the next operating cycle and decision making intended to benefit future periods is foregone. Basically, the long-term economic health of the organization is left to chance in lieu of meeting short-term expectations, particularly those of the owner. Investment in employee development (training) is the first victim of the budgetary axe. In the past two years the NIGC has found through comprehensive Minimal Internal Control Standards (MICS) audits that 38 percent of those audited had inadequate Title 31 training programs. Experience has demonstrated that when front line casino staff is not provided the necessary training to be effective in their positions, discontent results, which in turn produces higher turn-over rates, which in turn increases the need for more training and results in a general decline in the quality of governance programs. Furthermore, it has not been uncommon for management to reduce personnel in non-revenue producing areas. For example, cashier, revenue audit, internal audit, and accounting and payroll positions have all become increasingly vulnerable. We believe the degradation of many BSA compliance programs results from scaled back employee training and staff reductions, which increases the risk of gaming operations becoming a pawn in money laundering schemes. Furthermore, as casino management is well aware, individuals possessing the desire to bring the appearance of legitimacy to monies acquired through nefarious means are unwelcome guests. These people are criminals and pose a risk to the reputation of the industry.

Gaming has changed dramatically over the past decade. Technological advancements have been both cure and curse and now the overall market is shrinking. Ensuring that a gaming operation continues to maintain market share but simultaneously balances operating expenses with the revenue stream produced is a task of management requiring optimal skill. During tough economic times, our free enterprise system is exceedingly effective at weeding out the less capable operators and those facilities that are undercapitalized. Tribes that short change the needs of their gaming operation and whose management lacks competency to rise to the occasion of responding to the current challenges will find profits harder to find, increasing levels of waste and abuse, and their good governance programs crippled. Organizations in which tribal government officials and management have recognized the need to maintain sufficient liquidity to ensure operational effectiveness, assure funds are available to timely retire debt, and protect the capacity of their internal control systems will be poised to take advantage once the economy rebounds.



Section 6 - Feedback Form

Financial Crimes Enforcement Network U.S. Department of the Treasury

Your feedback is important and will assist us in planning future issues of *The SAR Activity Review*. Please take the time to complete this form. The form can be faxed to FinCEN at (202) 354-6411 or accessed and completed online at <http://www.fincen.gov/feedback/fb.sar.artti.php>. Questions regarding *The SAR Activity Review* can be submitted to sar.review@fincen.gov. For all other questions, please contact our Regulatory Helpline at 1-800-949-2732. Please do not submit questions regarding suspicious activity reports to the SAR Activity Review mailbox.

A. Please identify your type of financial institution.

Depository Institution:

- Bank or Bank Holding Company
- Savings Association
- Credit Union
- Foreign Bank with U.S. Branches or Agencies

Securities and Futures Industry:

- Securities Broker/Dealer
- Futures Commission Merchant
- Introducing Broker in Commodities
- Mutual Fund

Money Services Business:

- Money Transmitter
- Money Order Company or Agent
- Traveler's Check Company or Agent
- Currency Dealer or Exchanger
- U.S. Postal Service
- Stored Value

Casino or Card Club:

- Casino located in Nevada
- Casino located outside of Nevada
- Card Club

Dealers in Precious Metals, Precious Stones, or Jewels

Insurance Company

Other (please identify): _____

B. Please indicate your level of satisfaction with each section of this issue of *The SAR Activity Review- Trends Tips and Issues* (circle your response).

1=Not Useful, 5=Very Useful

Section 1 - Director's Forum	1	2	3	4	5
Section 2 - Trends and Analysis	1	2	3	4	5
Section 3 - Law Enforcement Cases	1	2	3	4	5
Section 4 - Issues & Guidance	1	2	3	4	5
Section 5 - Industry Forum	1	2	3	4	5
Section 6 - Feedback Form	1	2	3	4	5

C. What information or article in this edition did you find the most helpful or interesting? Please explain why (please indicate by topic title and page number):

D. What information did you find least helpful or interesting? Please explain why (again, please indicate by topic title and page number):

E. What new TOPICS, TRENDS, or PATTERNS in suspicious activity would you like to see addressed in the next edition of *The SAR Activity Review – Trends, Tips & Issues*? Please be specific - Examples might include: in a particular geographic area; concerning a certain type of transaction or instrument; other hot topics, etc.

F. What questions does your financial institution have about *The SAR Activity Review* that need to be answered?

G. Which of the previous issues have you read? (Check all that apply)

- | | |
|--|--|
| <input type="checkbox"/> Issue 1 - October 2000 | <input type="checkbox"/> Issue 2 - June 2001 |
| <input type="checkbox"/> Issue 3 - October 2001 | <input type="checkbox"/> Issue 4 - August 2002 |
| <input type="checkbox"/> Issue 5 - February 2003 | <input type="checkbox"/> Issue 6 - November 2003 |
| <input type="checkbox"/> Issue 7 - August 2004 | <input type="checkbox"/> Issue 8 - April 2005 |
| <input type="checkbox"/> Issue 9 - October 2005 | <input type="checkbox"/> Issue 10 - May 2006 |
| <input type="checkbox"/> Issue 11 - May 2007 | <input type="checkbox"/> Issue 11 - October 2007 |
| <input type="checkbox"/> Issue 13 - May 2008 | <input type="checkbox"/> Issue 14 - October 2008 |
| <input type="checkbox"/> Issue 15 - May 2009 | <input type="checkbox"/> Issue 16 - October 2008 |

The *SAR Activity Review* **Index** is now available on the FinCEN website at:

http://www.fincen.gov/news_room/rp/files/reg_sar_index.html

For your convenience, topics are indexed alphabetically by subject matter.

The **Archive of Law Enforcement Cases** published in *The SAR Activity Review* can be accessed through the following link:

http://www.fincen.gov/news_room/rp/sar_case_example.html

