GREAT AMERICAN and LOWERS RISK GROUP

Issue #41

February 2016

The Casino Shield

TITO Machine Mishap

Sometimes the employees who you can depend on the most to perform their routine functions efficiently are the ones who are taking advantage of your trust. This was the case with a mid-sized casino with a long-time, trustworthy staff that helped it run successfully for years.

TITO (ticket-in, ticket-out) systems are very popular for gaming operations as they streamline the cash out process and eliminate the need for coins, which are nearly obsolete. For smaller, more frequent payouts, TITO kiosks are a modern solution for the automated world in which we live. While internal controls over employees and built-in controls with these machines deter theft, fraudsters always seem to find a way to steal, especially when working as a team.

During a routine refill procedure of a TITO machine, a supervisor noticed a previously marked defective cassette on a cart with other cassettes which was on its way to be refilled at a kiosk. The supervisor happened to see this and luckily stopped this defective cassette before it was mistakenly loaded into the kiosk. To make sure this wasn't causing any cash discrepancies, the defective cassette was brought to the main bank room where a hand count was performed. It was found that the cassette was missing money. This raised concerns and an unscheduled count of all cassettes in all of the kiosks was performed immediately. The concerns were validated as additional cash was found to be missing. The casino realized they had a serious problem that needed a solution as soon as possible so they began monitoring surveillance footage extremely closely for the next week.

They noticed two main bank employees using a counting machine as they normally would, but instead of following usual procedures, the employees began separating out stacks of bills and setting them aside in drawers or other suspicious places. This money was never used to fill the kiosks. The suspicious activity continued as they observed one employee give a stack of cash to a cocktail waitress, who turned out to be the employee's sister. The cocktail waitress then placed the money in her locker and later handed the money off to a casino patron accomplice who walked out with it. The total amount of money documented as withdrawn from the main bank was not all deposited in the kiosks and the records submitted by the employees were falsified to indicate that all the money was placed in the kiosks.

The full investigation revealed this scheme went on for about 8 months and over $750,000 was stolen. The three employees, who were very well liked and had all been employed for over 8 years, were arrested and convicted. The accomplice was arrested and convicted as well. Had it not been for the supervisor being in the right place at the right time and noticing a defective cassette, the scheme could have continued longer resulting in an even larger loss. The lesson here is that while new technology has embedded security features, it should not replace routine, unscheduled audits and surveillance monitoring of employee activity. This includes all employees, even those who are above average performers and long tenured.

The above narrative is fictional; however, it is based on situations that have been reported.

By Patrick Shannon, Sr. Account Executive
Great American Insurance Group
Fidelity / Crime Division

Contact List

Great American is prepared to provide the insurance protection your casino needs to guard against fraud, theft, robbery, kidnap and ransom, or computer crime. For more information, please contact:

Stephanie M. Hoboth
Senior Vice President
(860) 285-0076
smhoboth@GAIC.com

Trust your risk mitigation needs to Lowers Risk Group, an independent, internationally recognized provider of loss prevention, investigation, and enterprise risk management (including human capital risk) services to the Casino & Gaming Industry. For more information, please contact:

Steve Yesko, ARM
Director, Business Development
(540) 338-7151
syesko@lowersriskgroup.com

Inside This Issue

Not If But When: How to Avoid Becoming the Next Target of FinCEN AML Enforcement

Background: Anti-Money Laundering (AML) compliance is becoming more complex and demanding for a wider range of industries. Regulators have increased their scrutiny and fines have been levied on businesses outside of the traditional financial institutions space, including casino and gaming operations as well as Money Services Businesses (MSBs). The good news is that these non-FI organizations can apply many of the best practices from the financial services sector to help meet regulatory requirements without driving up costs or compromising the patron experience.

If you run a business that facilitates or conducts money transactions, or transactions in other liquid commodities, you are no doubt aware of FinCEN. Rest assured that FinCEN is aware of you, too. And we predict it's only a short matter of time before their foreshadowing of AML enforcement actions against the cash servicing and transport industry becomes a harsh reality.

The Financial Crimes Enforcement Network (FinCEN) is the arm of the U.S. Treasury charged with investigation and enforcement of Bank Secrecy Act provisions intended to block the financial sources of illegal and terrorist organizations. Traditionally, the BSA applied to common financial institutions like banks and credit unions. But as banks began to offload services to third party vendors and the number of money-related businesses like check cashers and wire transfers proliferated, the BSA has been applied to an ever-wider array of businesses.

Many of these newer businesses are collectively known as Money Service Businesses (MSB). Businesses that transmit money, issue money orders, cash checks, deal in foreign currencies, or a number of other types of transactions, are required to register with FinCEN and maintain an effective Anti-Money Laundering (AML) program.

We recently summarized a presentation FinCEN gave to the Secure Cash & Transport Industry last October. Alan Cox, Acting Associate Director of the Liaison Division for FinCEN, sent a very clear and powerful message to the industry: Comply with AML requirements or face significant enforcement actions.

Exemptions are Few and Far Between

Cox explained that the exemptions to FinCEN rules are extremely narrow, specifically with respect to currency transportation. A currency transporter can be exempted from FinCEN if it has ONLY a custodial interest in the currency or other valuable. But the conditions that define what is "custodial" are very limited and precise.

The Treasury and its implementing laws aim to throw a broad net over currency transactions, and use the resulting data in numerous legal investigations. Some recent FinCEN enforcement actions show that the agency defines MSB broadly, includes even small businesses, and takes punitive action when it deems a business is out of compliance:

- **B.A.K. Precious Metals, Inc.** received a civil money penalty of $200,000, December 2015: Failed to establish and maintain an effective AML program for its precious metals business despite repeated compliance reviews; failed to assess or monitor clients; failed to report transactions.

- **Oaks Card Club** received a civil money penalty of $650,000, December 2015: Failed to establish an effective AML program for its gambling business;

Continued on page 3

Continued from page 2

alerted customers when they were about to pass the $10,000 threshold requiring a currency transaction report (CTR); failed to file suspicious activity reports (SARs).

- **Lee's Snack Shop** received a civil money penalty of $60,000, June 2015: Failed to establish and maintain a compliance program; failed to conduct adequate testing; failed to file currency transaction reports.

- **King Mail & Wireless** received a civil money penalty of $12,000, June 2015: Failed to establish an effective AML program for its money wire transfer business; failed to file suspicious transaction reports.

- **Ripple Labs Inc.** received a civil money penalty of $700,000, May 2015: Failed to register as a Money Service Business; failed to establish an AML program for a virtual currency (Ripple); failed to file suspicious activity reports.

- **Aurora Sunmart Inc.** received a civil money penalty of $75,000, March 2015: Failed to re-register the check cashing service as an MSB on a timely basis; failed to establish an effective AML program; failed to report transactions over $10,000; failed to establish effective internal controls.

If there is even a remote chance that your business is a Money Service Business, look at the FinCEN requirements and determine if you should be registered with FinCEN. If your business is an MSB, you could face significant penalties for failure to comply.

Learn more about how to ensure your compliance by referencing our last article on this topic, "FinCEN's Alan Cox Foreshadows AML Enforcement Actions in Armored Car Industry Address".

About The Author

Lowers Risk Group provides comprehensive enterprise risk management solutions to organizations operating in high-risk, highly-regulated environments and organizations that value risk mitigation. With Lowers Risk Group you can expect a strategic, focused approach to risk assessment, compliance, and mitigation to help drive your organization forward with confidence. Give us a call today to learn how we can help your organization or visit us online at www.lowersriskgroup.com.

16 Fraud Facts to Fuel Your 2016 Prevention Planning

As we begin 2016, we thought it might be useful to get a quick big picture on organizational fraud for context. We have been posting about the causal factors driving fraud and urging you to develop an effective risk-based prevention program. Now, here's the why — 16 facts about fraud drawn from the 2014 ACFE Report to the Nations that should make it relevant to you.

1. Overall, survey participants estimated that organizations lose about 5% of top line revenue every year. That's $3.7 trillion in 2013 Gross World Product (GWP).
2. The median loss for a fraud episode was $145,000, but that conceals a wide variation in amounts. 22% of cases cost $1 million or more.
3. The median duration of a fraud — the length of time between inception and detection — was 18 months.
4. Asset misappropriation was the most common of the three types of fraud, occurring in 85% of reported cases and costing a median $130,000. The least common type was financial fraud at 9%, but these were extensive thefts with a median loss of $1 million. In between, corruption occurred in 37% of cases at a median cost of $200,000.
5. 30% of the reported frauds involved more than one type of fraud.
6. Over 40% of cases were finally detected through a tip, about half of which were from an employee.
7. Organizations with hotlines were more likely to uncover a fraud by a tip.
8. Organizations of all sizes and types experience fraud — for profit, not for profit, government, and in all industry sectors.
9. Smaller organizations suffer disproportionately larger losses than larger organizations.
10. Fraud varies by industry, with financial services, government, and manufacturing having the greatest number of cases, but with losses per case higher in mining, real estate, and oil and gas.
11. Anti-fraud controls work. Organizations reporting fraud that had these controls in place experienced smaller losses and shorter duration of a fraud episode.
12. Fraud occurs at all levels of the organization, including employees, managers, and owners/executives.
13. The more authority held by the fraudster, the greater the losses.
14. Collusion helps fraudsters evade controls. The losses from fraud schemes increased as the number of people involved increased.
15. Certain departments were reported as more susceptible to fraud — accounting, operations, sales, executive/upper management, customer service, purchasing, and finance.
16. Recovering losses was slow and uncertain. Only 14% of participants had recovered ALL losses, and 58% had recovered NONE at the time of the survey.

Request a meeting with a Lowers Risk Group consultant to find out more about how your organization can fight fraud.

Three Charged in Casino Fraud Case at Mohegan Sun Pocono

January 20, 2016: By James Halpin—citizensvoice.com

Plains Township -- The former vice president of player development at Mohegan Sun Pocono was charged Tuesday with conspiring with a cocktail server and a frequent gambler to defraud the casino out of hundreds of thousands of dollars, facing 177 counts including theft, identity theft, criminal conspiracy, winning by fraud, computer trespassing, and misapplying trusted property.

The scheme, which was referred to as a "handshake," involved the cocktail waitress collecting players' cards and PIN numbers as she served drinks, and then passing them on to the VP. He in turn created duplicate cards and added free slot money on each one before giving them to the frequent patron, who in turn used the cards at the casino slot machines and split his winnings with his two co-conspirators. Although patron cards were used in the scheme, it is believed that no customers lost any of their expected free slot play.

A review by the casino determined that the scheme was in operation from May 2014 through April 2015 and included $478,100 in free gaming credits that generated $418,793 in winnings, including four jackpot wins of $2,000 each.