



DATA ANALYTICS: WHAT YOU DON'T KNOW CAN HURT YOU

By Brian Lopez

Casinos are often action packed with all types of sights and sounds from slots to table games, enough to cause sensory overload. But behind the glitz and glamour of a casino, there is a virtual sea of data being generated every second. The amount of data generated in a casino can be staggering, especially if you are tasked with analyzing that data. Nowadays, mentions of “Big Data” and its associated analysis are ubiquitous in publications and postings, but it is a vital part of making sure a casino is safe from money laundering threats, fraud, and other issues. Data can tell you all types of stories about a casino. Specifically, it can uncover Title 31 systems issues, potential procedural and internal control issues, data integrity flaws, and other types of money laundering threats. Marketing departments have been using gaming data to analyze player activity patterns for years, yet compliance departments rarely use or analyze the data that is available to them. So, if you don’t know your data, you don’t know your customers and you don’t know the potential threats to your operation.



Potential Title 31 System Issues

Presently, most casinos are using some kind of Title 31 software to help them gather and aggregate the data that is generated on a daily basis. For example, bills inserted into slot machines, vouchers cashed-out at ticket redemption machines, cash buy-ins at tables and transactions happening at the cage are some of the transactions usually captured by a host data system. The data generated from the host systems is then transmitted to a Title 31 software program, enabling the users of the program to have a 50,000-foot view of the activity in their casino. This Title 31 software helps the user aggregate cash transactions throughout the casino during the gaming day to be used for regulatory reporting. Also, the Title 31 software supplies the user with data to analyze for patterns of potentially suspicious activity. If a casino is using a Title 31 software, they should make sure they have an answer to one critical question –how do you know if the Title

31 software has all the data? In a home or building with a complex array of plumbing pipes, how do you know if you have a leak, especially if a pipe is out of plain view? The disparate host data systems of a casino feeding into the Title 31 software can pose the same type of problem if there is data leakage somewhere. This could be a serious problem and have a significant impact on regulatory reporting for Currency Transaction Reports (CTRs) by underreporting aggregate cash amounts or failing to file a report altogether. Absent transactions could be the missing link for the identification of patterns of suspicious activity, and conversely the missing transactions could help clarify situations that were previously deemed as suspicious. To the extent transactions were missed, this could lead to a “lookback” whereby the casino has to go back over a period of time and determine all regulatory reporting that may have been incorrect or missed. Needless to say, the undertaking necessary to conduct a lookback can be extremely time consuming and expensive.

There are a variety of potential causes for data leakage, such as software upgrades of host systems or improper software setup and installation. To help identify any potential issues with your systems, you should conduct a data flow analysis. Simply put, a data flow analysis compares the data housed in the host system against the data stored in the Title 31 software system. Data flow analyses should be conducted on any system that integrates with Title 31 software, especially after any type of system upgrade or new system implementation. Conducting an effective data flow analysis can prevent regulatory headaches, especially for the compliance department, that could result in civil monetary penalties.



Procedural or Internal Control Issues

In addition to Title 31 software issues, casino data can also help to identify potential procedural or internal control problems. As an example, table game ratings are imperative to capture cash buy-ins or chip purchases with cash. The Title 31 software consuming

this rating data, as well as the user analyzing the data, relies on the individual inputting rating data to be complete and accurate. But what if the data is inaccurate or missing key information? If critical rating information is omitted or input in error, the Title 31 software may misrepresent information to the user. This again could have an impact on regulatory reporting and the identification of potentially suspicious activity.

A critical element of both slot and table rating data is capturing the cash activity on the proper gaming day. For regulatory reporting of CTRs, cash activity needs to be aggregated by patron for a 24-hour period, often referred to as the gaming day. Aggregated cash activity for either cash-in or cash-out transactions exceeding \$10,000 in the 24-hour gaming period needs to be reported by filing a CTR. As such, the compliance team needs to rely on an accurate rating date, as well as the beginning and ending times of the ratings for the proper filing of a CTR. If the rating date or times are inaccurate or if a rating is not closed on time, the gaming date represented in those transactions will be incorrect. This will result in an incorrect CTR.



Data analytics can be leveraged to ensure ratings are complete and accurate. By analyzing the dates and times of ratings, you can ensure that critical data elements are not being missed or misrepresented. Summarizing slot and table ratings by other information stored in the ratings data can help to uncover these potential issues. As an example, you can isolate all ratings missing key information by physical location, game type, employee shift or employee ID to see if the potential issues have a pattern. Are my incorrect ratings associated with a particular pit location? Are my incorrect ratings associated with a particular pit manager or shift? Analyzing your rating data in this manner can help uncover potential procedural or control issues that may have gone unnoticed and can help lead you to the root cause of the problem.



Data Integrity

As mentioned in the previous section, reliance on correct data is imperative to ensure regulatory reporting is accurate and to help with the identification of suspicious activity. In many Title 31 systems, a gaming date is created once the data from the host system is input, whereby the Title 31 system calculates the gaming date based on date and time the information was sent from the host system. So, how do you know if the gaming date is being calculated correctly by the Title 31 system? If the gaming date calculation is off, the domino effect of incorrect reporting issues previously mentioned could occur. Using data analytics to ensure the accuracy of the gaming date calculation is a best practice in the gaming industry.

While the gaming date is a critical element in aggregating cash activity for the 24-hour gaming period, the other critical element in cash aggregation is a patron identifier, commonly referred to as a patron number or patron ID. The patron identifier is usually tied to a player reward system whereby marketing can track patrons' gameplay. So, how do you know that your patron ID is accurate? How do you know if a patron has multiple IDs? There could be instances where a patron is issued another ID inadvertently, or instances where a host system issues an ID with a different schema. Regardless of how it may happen, leveraging data analytics to identify these issues is key. Summarizing the patron master file or Multiple Transaction Log (MTL) by patron ID and another key identifier, such as a social security number or a driver's license number could help to identify these types of issues.



Identifying Suspicious Activity

As criminals continue to utilize casinos as a means to launder or disguise illegally derived funds, compliance professionals can use the data generated in the casino to detect potentially suspicious patterns of activity. Given the sheer volume of data generated in a casino, leveraging data analytics to identify particular indicators and patterns is an absolute must in this digital age. The Financial Crimes Enforcement Network (FinCEN) has issued guidance for casinos and compliance professionals to help identify various types of red flags. At a minimum, compliance professionals should be looking for indicators related to structuring (avoiding CTR reporting), minimal gaming activity, large cash-in or cash-out activity without game play, and chip walks (patrons leaving the casino with large amounts of chips). Given that not all casinos have the same types of risks, analytics looking for these types of potentially suspicious activity should be tailored accordingly. As an example, a large Las Vegas casino may be seen as more of a destination casino offering different types of games at different dollar limits with patrons gambling for only a few days at a time. On the other hand, smaller casinos located outside major cities are more likely to be considered a “locals casino” with fewer games and a population of patrons who attend the establishment regularly. These two types of casinos are different and as a result have different types of money laundering risks. Given these different types of risks, data analysis thresholds and variables used to identify suspicious activity at each type of casino will vary. So, there is no “one size fits all” approach, but given the power of data analysis, compliance professionals can tailor their analytics accordingly. Furthermore, regulators are starting to employ data analytic techniques more frequently during examinations of a casino’s anti-money laundering program. As such, compliance professionals should leverage data analytics to ensure they do not miss potential red flags.



Conclusion

In order to be effective in the use of data analytics, compliance professionals need to make sure they have the proper training and the tools to get the job done. Computers are getting smaller, cheaper, and faster every day. This means that users now have the ability to analyze 100% of data populations rather than a random sampling, making suspicious patterns and red flag indicators easier to identify. Given the explosion of big data and analytics in recent years, there is no shortage of resources available to help compliance professionals become more proficient in the use of data analysis techniques. Having a basic foundation in the understanding of data and how relational database systems work is vital. Couple that knowledge with software that can help you interrogate all types of digital information and you have the keys to unlock a powerful story that your information may be trying to tell.



Brian Lopez is a Director with the Dowling Advisory Group where he specializes in the use of data to help all types of financial institutions to prevent money laundering and the funding of terrorist activity. Brian has worked with some of the largest casinos in the world, assisting with the independent testing of BSA/AML programs, remediation related to look backs, and data flows and BSA/AML system validations. Brian also regularly presents, writes, and instructs on the topic of forensic data analysis. He graduated from the University of Washington with a Bachelor’s degree in Industrial Engineering and obtained his Master’s in Business Administration from the UCLA Anderson School of Management. Brian is a Certified Fraud Examiner and a Certified IDEA Data Analyst.