

CGi

Casino & Gaming International





25



29

FEATURES

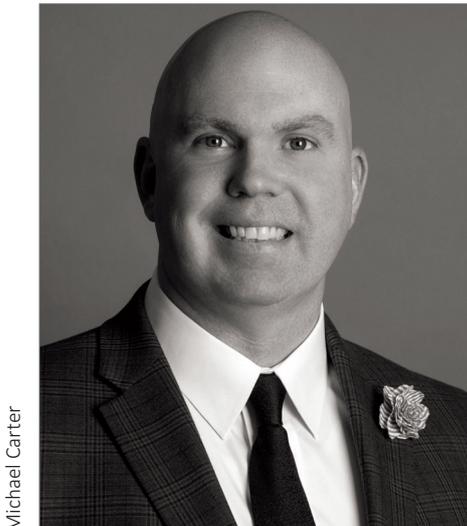
- 9
BREAKING THE CYCLE AND BUILDING LOYALTY IN iGAMING
 Dominic Le Garsmeur, SG Digital
- 11
GAMING IN THE DIGITAL AGE: GAMING EXPANSION AND RISK CONSIDERATIONS
 Elise Lebourg, Bob Boyle & Christophe Grippa, Ernst & Young
- 17
BEPS 2.0 - TAXATION OF DIGITALISED BUSINESSES?
 Adam Polacsik & Osarugue Obayuwana, KPMG Malta
- 21
CROSS-BORDER EXPANSION FOR THE EUROPEAN REMOTE GAMBLING INDUSTRY: THE LABYRINTH OF INTERNATIONAL TAXATION
 Andrea Ricci, Bellerophon Overseas
- 25
SOCIAL MEDIA FOR GAMBLING OPERATORS
 Melanie Ellis & William Reade, Northridge Law
- 29
THE CHANGING LANDSCAPE OF THE eGAMING INDUSTRY
 Interview with Lyle Wraxall, Isle of Man Digital



FEATURES

- 33** HOW 'LIVE CASINO REDEFINED' IS PAYING OFF
Amy Riches, Evolution Gaming
- 37** 'KICKING THE TIRES' ON GAMING COMPLIANCE PROGRAMS
Michael Carter & Lindsey Hallett, Alvarez & Marsal Financial Crimes
- 41** THE DEVELOPMENT OF ELECTRONIC TABLE GAMES IN THE UNITED STATES MARKET
Robert J. Baldassarre & Lea Giosa O'Neill, Fox Rothschild
- 45** GETTING IT RIGHT IN THE USA
Alessandro Fried, BtoBet
- 57** INNOVATION IN GAMBLING RESEARCH
Dr. Mark Griffiths, Nottingham Trent University

‘KICKING THE TIRES’ ON GAMING COMPLIANCE PROGRAMS



Michael Carter

Michael Carter & Lindsey Hallett

Alvarez & Marsal Financial Crimes

The gaming industry is expanding and gaming companies are growing their businesses in new markets with new players through a growing number of betting and entertainment products. Having peaked at almost \$42 billion in 2018, the US gaming industry has not yet observed the regulatory tail that may follow in this rapidly evolving environment. Understanding the new compliance risks presented by changing business components is essential to avoiding the repercussions that often result in regulatory enforcement, monetary penalties, business interruption, and reputational downgrade. These new compliance risks span money laundering, fraud, corruption, cybersecurity, and data privacy and security, to name only a few. Regularly testing compliance functions for gaps in controls, data, change management, processes, and outcomes is likely to enable further, less-impeded growth and serve as a market differentiator for gaming companies who get compliance right.

In April 2019, the Department of Justice specified its perspective through its “Evaluation of Corporate Compliance Programs” guidance, that outlines questions companies must ask themselves:

“Has the company reviewed and audited its compliance program in the area relating to the misconduct? More generally, what testing of controls, collection and analysis of compliance data, and interviews of employees and third parties does the company undertake? How are the results reported and action items tracked?”

For gaming companies, potential misconduct and compliance risks present themselves when new variables (players, employees, products, services, technology, and



Lindsey Hallett

jurisdictions) enter the picture in mass or rapid fashion; exactly what the gaming, sports betting, and casino industry is experiencing in 2019.

The Big Picture

Although based in regulatory guidance, every compliance program is different, so there is no one-size-fits-all approach to testing and validating the effectiveness of controls. Controls are derived from risk assessments which are unique to each company and require planned, regular testing to ensure the results are matching up to desired risk mitigation goals. When testing and validating the effectiveness of compliance program functions, it is important to keep in mind the following overarching concepts:

- Ensuring what is documented in policies, procedures, and risk assessments matches the description and functions of the program controls;
- Documenting the regulatory basis for each control and related changes and updates;
- Assessing if the program functions are meeting the intent of the compliance requirements as outlined in regulations and law;
- Determining if the performance expectations are documented and current;
- Assessing whether performance outcomes are sustainable based on current resources; and
- Understanding the available data, and if that data confirms or denies compliance performance measures.

Starting with Data

Bad data in, bad decisions out. It is extremely difficult to make risk decisions at operational and strategic levels if the information and data are compromised throughout the data lifecycle. Data testing provides compliance leaders the opportunity to assess the completeness and accuracy of data inputs, specifically regarding player information and

recordkeeping, gaming activity and behavior patterns, and completeness of reports.

In August, FinCEN Director Kenneth Blanco highlighted increases in Minimal Gaming with Large Transactions and Chip Walking activity in recent Suspicious Activity Reports. Quality end-to-end data process flows are vital to identifying and reporting this type of activity and understanding the trends that may warrant updates to controls to reduce unusual or suspicious activity. Robust KYC information profiles, consistently collected, accessed, and updated, can help in developing linkage between players involved in suspicious activity.

Considerations in testing and validating compliance data include:

- Reviewing completeness and accuracy of data inputs and outputs (performance metrics, rules, and information quality);
- Checking if data is formatted consistently from source to output, and is robust enough to enable meaningful analysis;
- Assessing the interoperability of data among IT systems, through business units, and across geographies;
- Ensuring that data flows and processes are documented accurately;
- Ensuring data is stored, protected, and segregated in accordance with regulations, policies, and procedures. This includes “Red Teaming” to test against security, manipulation, and penetration risks from a cybersecurity perspective, as well as ensuring data is being used in accordance with local customer data privacy requirements;
- Understanding remote and online remittance data, including risks associated with masking or circumventing IP restrictions (especially for mobile gaming); and
- Testing if the analysis derived from data is accurate, meaningful, and applicable to executive management’s compliance guidance.

In May 2018, FinCEN issued Enforcement Action Number 2018-02 which included data-related Anti-Money Laundering failures of a card club, specifically highlighting the lack of use of automated data “systems to aid in assuring compliance.” In this case, instituting even a basic level of data testing, in combination with transaction monitoring controls, may have enabled the casino to identify “multiple transactions at or just below \$10,000” and be able to demonstrate examinations and reasonable dispositions of suspicious transactions. Data may not be the “end-all and be-all” of compliance, but it certainly touches every component of a quality program.

More recently, there has been a class action lawsuit within the Ontario Superior Court of Justice related to the stolen data of customers, employees, and suppliers via a casino-entertainment company and the Ontario Lottery and Gaming Corporation. While the matter is ongoing, it certainly hints at how liable or negligent gaming entities may be perceived without proper data protections and robust testing.

Adequate Resources

Compliance programs can ultimately be broken down into functions of people, processes, and technology. As with any endeavor, getting the people component right possesses a unique complexity and approach that requires deliberate

planning, attention, and supervision. Compliance staffing often serves as a primary cost center, though the people making up that cost center may also be viewed as the primary compliance resource. Again, the casino and gaming industry is expanding so rapidly that the normal requisite industry-specific experience sometimes has to be substituted for robust training and compatible cross-industry expertise. This unique situation also warrants special attention to testing the efficacy of compliance staffing while simultaneously enabling them to carry out smart, risk-mitigating measures. With regards to establishing the effectiveness of the investment in compliance personnel, review considerations include:

- Ensuring the size of compliance staff is commensurate with company size and activity, and is upwardly scalable as operations grow;
- Onboarding and training compliance professionals with appropriate experience and enabling cross-functional overlap of expertise (for example: table games and slots, sports book, bingo, and cage operations);
- Dedicating appropriate resources, time, and money to training teams across the organization in addressing the variety of compliance risks;
- Appropriately focusing compliance staff on high-risk operations and functions; and
- Ensuring that compliance officers are adequately enabled to address control risks and effectiveness concerns.

Transaction and Player Monitoring

Depending on the type of risk being addressed, monitoring can be very nuanced and a real challenge from a testing standpoint. Common approaches for validating detection systems include “Above/Below the Line” and statistical rule effectiveness tests. For customer screening, fuzzy logic and key term components of transaction and player attributes warrant regular updates and reviews to capture changes to detection avoidance typologies. Testing systems for effectiveness in capturing behavioral patterns may help identify, in part:

- Structured redemptions;
- High-value chip transfers;
- Chip walking;
- Chip manipulation, including RFID-defeat activities;
- Slot ticket-in, ticket-out schemes;
- Player collusion, including betting multiple or both sides of a table game, sportsbook wager, or fantasy contest;
- Unusual player interaction with employees;
- Using a casino cage for banking activities; and
- Other fraudulent or illegal activity.

No matter the focus of the testing, it is important to consider the differences and potential gaps between automated and manual systems, the timeliness of alerts, incorporation of investigation outcomes into the monitoring system, cross-border transaction and player risk, and testing a system’s



resilience against unstructured, faulty, or manipulated data. It makes sense to periodically check that monitoring standards and production results match the Key Performance Indicators and are nested with the organization's risk assessments. Additionally, testing should address the documented process for changing monitoring standards, rules, and procedures.

Benchmarking

If compliance can be considered both an art and science, benchmarking probably leans more towards an art form. Comparing compliance functions to "best" or common practices is a handy tool to identify pitfalls across the compliance landscape. Conducting an internal comparison of performance indicators between functions can be helpful in identifying both what is working elsewhere within the same company, as well as redundant activities that could enable the reallocation of resources. When relying on external benchmarking approaches, key questions to ask are:

- Is expert judgment being relied on as a basis for compliance practice reasoning? If so, does that judgement still apply based on the operating environment, the risk assessment, and internal operations?
- Is there a plan to address residual risk, or risks of a system failure when mirroring outside compliance approaches?
- Who is defining "best practices"?
- How long is this benchmark system valid in its current state? Are there any known or planned changes to strategy, environment, resources, personnel, or risks that would limit the applicability or effectiveness of the program function?
- Are all policies and procedures relating to this benchmark up to date and stored in accordance with company procedures? Has all reasoning behind the compliance decisions based off benchmarks been documented?
- Are the compliance benchmarks achievable and aligned with business strategy, player experience goals, and the budget?

Other Internal and External Considerations

Other compliance gaps may present themselves when control functions don't quite fit neatly into a particular bucket. Common components of high-functioning programs that may be overlooked include:

- Balancing customer/player experience with regulatory and legal requirements;
- Employee screening and monitoring;
- Third-party screening and monitoring;
- Level of ownership, responsibility and authority, of key compliance functions; and
- Gaps in communication among and between departments, especially for marketing and entertainment business units as they relate to compliance.

Triggers to Test

So, when should you conduct testing and validation exercises? The best answer is "always," but that really just means you should always be monitoring compliance risk. In the spirit of applying feasible, defensible concepts to effective compliance programs, there are a few event-oriented triggers to track that may warrant a review for controls effectiveness:

- Changes in risk appetite or strategy by senior management;
- Significant changes to the residual risk derived from the risk assessment;
- Updates to regulatory guidance;
- Trend changes in customer/player profiles, geographic concentrations, or activity;
- New product offerings;
- Entering new markets;
- Expansion of pilot compliance initiatives;
- Changes in technology; and
- Identification of severe or multiple compliance failures.

In short, the scope and frequency of independent testing and validation must be commensurate with risks confronting the businesses... from a periodic and an event-based approach.

Final Thought

Ultimately, conducting effective, planned testing and validation activities allows senior management, board members, and compliance staff to answer: "Does our compliance program work?" In defining what "work" means in the gaming industry, it can be helpful to keep in mind the potential pitfalls that run throughout compliance risk assessments, planning, implementation, and operations:

- Testing the wrong functions, data, or at the wrong risk level;
- Incomplete testing which leads to making incorrect conclusions about compliance effectiveness;
- Interpreting testing and validation outcomes incorrectly... "painting targets around the arrows";
- Key controls derived from the risk assessment have not been comprehensively addressed in the testing and validation plan; and
- Significant assumptions or reasoning behind management operations, guidance, or policy and procedure remain unconfirmed. **CGI**

MICHAEL CARTER & LINDSEY HALLETT

Michael Carter is a Senior Director with Alvarez & Marsal Financial Crimes and Investigations in Washington D.C. He specializes in Anti-Money Laundering, Counter-Terrorism Financing, sanctions, fraud, bribery and corruption. Mr. Carter brings more than 15 years of experience providing organizations with advisory, performance improvement, and operational and organizational leadership.

Lindsey Hallett is an Operations Manager with Alvarez & Marsal Financial Crimes and Investigations in Washington D.C. She specializes in providing operational support to clients, and possesses extensive knowledge of global compliance operations related to diversified financials, high-growth businesses, and emerging industries.