TRANSACTION MONITORING OF GAMING ROOMS: SOME CONSIDERATIONS

As a pub or a club with slot machines ('pokies'), multi-gaming terminals, cash redemption / ticket redemption terminals and cashiers, you are required to have a transaction monitoring program in place that will enable you to detect:

- Unusual transactions or patterns of transactions;
- Structuring (breaking large transactions into smaller ones to avoid reporting thresholds);
- Transactions with people in high-risk countries, or with people on a sanctions or politically exposed person (or PEP) list; and
- Unusual customer behavior which may indicate money laundering or terrorism financing.

AUSTRAC makes this clear in its guidance materials available here: Transaction monitoring | AUSTRAC

(…it is recommended that reporting entities have AUSTRAC's website as a 'favourite' to make sure you're up to date on their guidance materials!)

START WITH THE RISK ASSESSMENT

As 'reporting entities' under Australia's AML laws, pubs and clubs with gaming machines will have in place AML/CTF Programs that describe their process for assessing the ML/TF risks faced by the business, having regard to the nature, size and complexity of the business.

Known as the "Enterprise-wide ML/TF Risk Assessment", or your "EWRA" it should consider the following factors:

- **Customer Risk:** Who are your patrons and what risks do they present?
- **Product Risk:** Which services are most vulnerable to misuse?

- **Channel Risk:** How do customers interact with your gaming facilities? (how are the gaming services 'delivered'?)
- **Jurisdiction Risk:** Are there geographic risk factors (i.e. do you deal with foreign jurisdictions)?
- **Employee Risk:** How might staff be involved?
- **Location Risk:** Does your venue's specific location create its own risks? If you have more than one venue, how do their risks differ?
- **Threat Environment:** What current criminal methods are targeting venues like yours?

You should also have a clear assessment of the red flags or **typologies** that are common for the pubs and clubs' industry. There are several useful guides and resource materials that discuss potential ML/TF typologies associated with gaming machines. These include (without limitation):

- AUSTRAC's Regulatory Guide for Pubs and Clubs
- The 2024 AUSTRAC National Risk Assessment into Money Laundering and Terrorism Financing
- AUSTRAC's indicators of suspicious activity in the pubs and clubs' sector
- FATF's Guidance on vulnerabilities of casinos and the gaming sector
- The latest American Gaming Association Best Practices Guidelines

These publications are not exhaustive and should supplement any red flags or typologies you have identified as part of your EWRA.

If you have an existing AML/CTF Program, or EWRA, that you believe doesn't cover these factors, or your methodology isn't up to date (hasn't been reviewed in the last 12 months), please contact us.

KNOW YOUR TRANSACTION AND CUSTOMER DATA AND SYSTEMS

Now that you understand the nature of activity in your venues that could be indicative of ML/TF risks, it is important to assess:

- What data might be relevant – i.e. what data might indicate that ML/TF activity is occurring?
- What data is available to you?
- How do you access it?
- When do you receive it? i.e. is it real time, near real time, later?
- Are there any reliability issues?
- Do you need to process the data before it is useful?
- Is it complete or does it need to be supplemented?

When looking at what data might be relevant, a good place to start is considering the entry, flow and exit points in your venue that illicit money might take (for instance, cash insertion into a

gaming machine). In addition, think about which departments or employees might be best positioned to detect the entry, pathway and exit of such funds, and what systems do they use?

Remember: Poor quality, inaccurate or incomplete data leads to poor monitoring results.

ESTABLISH CLEAR TRANSACTION MONITORING RULES

For each monitoring activity, ask:

- Why am I reviewing this data?
- What specific suspicious activity am I looking for? Which risk factor does it sit under and/or which typology is this picking up?
- What makes a transaction unusual for our venue (or for this particular customer)?
- Am I combining multiple data sources? If so, how and why?

Clear rules help:

- Create consistency (across staff and venues);
- Allow appropriate resource allocation;
- Help management understand and approve the monitoring approach; and
- Prepare for technology solutions.

DATA + RULES = OPPORTUNITY FOR TECH ENHANCEMENT

A spreadsheet approach to transaction monitoring may be outdated for modern transaction monitoring ("*a 2006 solution to a 2025 problem*") – although always consider your business' size, scale and complexity.

Technological solutions, if properly considered, calibrated and integrated, can:

- **Automate data collection**: Pull information directly from gaming machines and internal systems;
- **Apply consistent rules**: Ensure all transactions are evaluated using the same criteria;
- **Reduce false positives**: Use more sophisticated algorithms ('rules'), informed by your risk assessment, to better identify truly suspicious activity;
- **Flag related transactions**: Connect activities across different machines or visit dates;
- **Generate comprehensive reports**: Create documentation for internal review and regulatory reporting;
- **Visualise patterns**: Present data in graphs and charts that make unusual patterns easier to spot; and
- **Scale with your business**: Handle increasing transaction volumes without requiring more staff.

When evaluating technology solutions:

- Ensure they are tailored for gaming venues, not just generic AML tools (it is not enough to merely 'plug in' a casino or financial services solution);
- Check they can integrate with your existing gaming systems;
- Confirm they include strong data privacy and security features;
- Look for flexible rule configuration that you can adjust as risks change; and
- Consider solutions that offer both automated monitoring and case management.

HOW DOES TRANSACTION MONITORING FEED YOUR RISK ASSESSMENT?

Your transaction monitoring program creates a valuable feedback loop for your risk assessment:

- **Review alert patterns**: Are you getting alerts for the risks you identified? If not, either the risk is not present, or your monitoring rules need adjustment;
- **Analyse investigation outcomes**: When you investigate alerts, document whether they represent genuine suspicious activity or false positives;
- **Track trends over time**: Note increases or decreases in specific types of suspicious activity, which may indicate changing risk patterns;
- **Compare across venues**: If you operate multiple locations, compare monitoring results to identify location-specific risks;
- **Adjust your controls**: Based on monitoring results, strengthen controls for confirmed risks and reconsider resources allocated to risks that aren't materialising; and
- **Document your findings**: Keep records of how monitoring results have informed changes to your risk assessment and control measures.

Remember that this process should be continuous - monitoring feeds risk assessment, which improves monitoring, creating an ongoing cycle of enhancement.

CONCLUSION

Effective transaction monitoring is not just a regulatory requirement for pubs and clubs — it is a critical component of your risk management framework.

By following the structured approach outlined in this guide, you can develop a robust transaction monitoring program that:

- **Aligns with your unique risk profile:** Every venue is different, with its own customer base, services, and operational characteristics. Your monitoring should reflect these specificities;
- **Leverages your data effectively:** Understanding what data you have access to, its quality, and how to interpret it makes the difference between a perfunctory program and one that actually detects suspicious activity;

- **Evolves based on findings:** The feedback loop between your monitoring and risk assessment ensures your program remains relevant and effective over time; and
- **Positions you for technological advancement:** As technology solutions mature for the pubs and clubs industry, having clearly defined rules and processes will make implementation more effective and less disruptive.

Remember that transaction monitoring is not just about ticking a compliance box - it is about protecting your business from being exploited for money laundering or terrorism financing. A well-designed program helps safeguard your reputation, avoid regulatory penalties, and contribute to the integrity of Australia's financial system.

Need assistance with your transaction monitoring program? Contact LCA today to arrange a consultation.

Lane Consulting & Advisory

20B Armstrong Street Middle
Park, Victoria 3206

0421 671 571

contact@laneconsultingandadvisory.com

https://laneconsultingadvisory.com