MRB Banking: The Critical BSA/AML Risk Assessment

Here's the next in our series about MRB banking: How to do it, how to not do it, and how to figure out whether you're doing it without knowing. In this installment, we discuss critical modifications to your institutional BSA/AML risk assessment that will guide your risk-based approach to MRB banking.

MRB business is regulatorily risky given the unsettled nature of federal regulation and it's risky from a money laundering perspective because of the large amounts of cash that pass though MRB businesses. This does not mean there are not very good reasons for financial institutions to consider banking MRBs. Managing the risks of banking MRBs is our purpose here.

Background

The very first step in managing anti-money laundering and terrorist financing risk is your creation of a current, formal BSA/AML risk assessment incorporating the breadth of your MRB banking program and the controls you will use to meet your business and regulatory obligations. If you strive for an efficient, risk-based BSA/AML program, the extra time you spend creating a complete, compliant risk assessment will pay dividends in limiting your business and regulatory risks of banking MRBs.

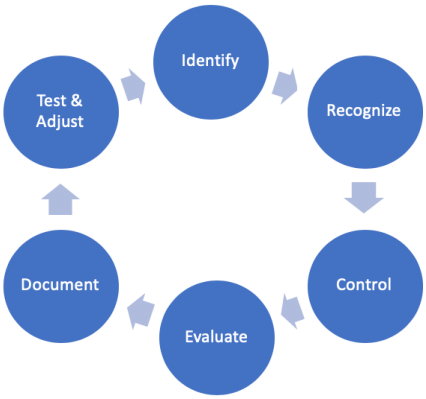
What does a compliant BSA/AML risk assessment look like? In general, the FFIEC BSA/AML Examination Manual is out of date, but its risk assessment principles are reasonably clear and applicable. The Conference of State Banking Supervisors (CSBS) published a manual spreadsheet that, while short on detail, gives a good sense of the principles state regulators see as critical to the risk assessment process.

A Complete Risk Assessment…the First Step

Any system of risk management starts with a risk assessment that follows the core principles of risk management. This means that you:

- **Identify** risks associated with your intended business through the development of *Key Risk Indicators*.
- **Assign** *Inherent Risk* of each *Key Risk Indicator*.
- **Outline** the *Controls* you will use to mitigate the *Inherent Risks*.
- **Evaluate and Report** the *Residual Risk*—the risk that remains after the proper application of the *Controls*.
- **Document** your evaluation of this process in a compliant risk assessment that meets the standers of the FFIEC's BSA/AML Examination Manual and industry best practice.
- **Test and Audit** your system of risk identification, risk assignment, and controls and adjust your risk assessment to account for documented risks.

Applying Risk Management/Assessment Principles to MRBs



Identify MRBs with which you are doing business.
It's not as easy as it sounds. We must recognize that MRB businesses know they have significant exposure to derisking and they are anxious not to disclose their association with cannabis. Many customers and potential customers might not lie, but they won't volunteer information. Thus, clear direct KYC inquiries along with connections to data sources that identify MRBs are critical. In addition, your KYC systems should include a check of licensing records for your state's MRBs (and near neighboring states if you are close to a border) to see whether your customer/potential customer is licensed as an MRB. There are very good third party services that will check not only records but identified principals of licensed MRBs, which is very helpful when you do beneficial ownership analysis.

Recognize MRB risk.
For the reasons discussed earlier in this paper, MRBs are inherently risky both from a regulatory and a business standpoint. You can't hide from that, so address it directly in your risk assessment. MRBs are inherently risky because they are often excluded from the traditional banking system and deal with cash or cryptocurrency, both of which can create anonymity in the revenue generating activities. The cannabis supply chain from growing to harvesting to processing to transportation to retail sales is driven largely at this point with cash or cryptocurrency, leading to potential difficulty identifying true transaction parties.

Control Accordingly: Control.
There are very good resources in the market today that help institutions manage MRB risk from transaction monitoring to KYC solutions. We have some ideas on what makes sense. Whether you ask us or discover your preferred vendors, use the resources available and implement real controls to mitigate MRB risk. These controls will be concentrated in two areas:

- CDD (including beneficial ownership analysis) and EDD and ongoing monitoring—more on this in a future installment
  and
- Transaction monitoring.

You likely have an automated transaction monitoring system and an adequate control structure around MRBs is incomplete without direct discussions with your monitoring partner and adjustment of your systems to account for the special challenges of banking MRBs. These adjustments include the recognition that MRBs are primarily cash-based businesses requiring scrutiny (above and beyond the typical cash based business) of transactions. Establishing a baseline of activity that fits the business profile is the first critical step to setting parameters for your monitoring system. For example, we expect retailers to make

very frequent, perhaps smaller, cash deposits commensurate with numerous small transactions. We might expect growers and processors to have much larger bulk transactions, but still within certain parameters that match their size and business profile. You should flag and investigate anything outside expected parameters.

Evaluate the effectiveness of your controls to determine residual risk.
Critical to the risk assessment process is your use of professional judgment to determine the effectiveness of the controls on the inherent risk to determine residual risk. At the outset, this is your best estimate of how the controls will mitigate inherent risk. But, as you go though business cycles and review red flags, investigations, CTR, SAR activity, ongoing EDD, and other data generated by your BSA professionals and your vendors, you will come to a reasonable, documented view of the effectiveness of your controls. Ongoing documentation of your evaluation of risk and the effectiveness of your controls will convince a reasonable auditor and examiner that you are continually addressing MRB risks in a best practice fashion.

Document your evaluation in a comprehensive written risk assessment.
It not is not enough to create and maintain a best practice risk assessment control structure. You must explain and document your reasoning to institutional leadership, auditors, and examiners. To do this, you must create a narrative risk assessment report which discloses each material risk, documents controls, and calculates residual risk.

Finally, test and react.
You've done everything right up to this point and then you apply the final step in best practice risk management. As a significant part of your ongoing risk management system, you must test and document the effectiveness of your controls, adjust your risk assessment to reflect where there is more or less than expected risk (based on factors such as red flags, investigations, SAR, and CTR activity), and revise controls to address unexpected risk. These control adjustments may be as simple as making changes to your monitoring system settings to sample more, less or different transactions in response to identified risk. This sounds simple, but many, many of your piers do not "finish the proverbial tackle" by changing their controls in reaction to risk. By the way, control changes can go both ways in that you might carefully reduce scrutiny on areas where you expected higher risk and found lower.

About the Authors

Mark Stetler is CEO of RegSmart. He has a BBA in Finance from Baylor University (cum laude, 1985) and a law degree from the University of Texas (with honors, 1988). Mark has worked in the financial services industry for 30 years as an attorney and entrepreneur and previously co-owned one the nation's largest firms specializing in forensic financial audits. He is a Certified Anti-Money Laundering Specialist and a chief architect of RegSmart's anti-money laundering risk assessment and audit SaaS.

Ben Knieff is an executive advisor and consultant, specializing in fraud detection, identity verification, authentication and biometrics, anti-money laundering, sanctions screening, counter terrorist financing, blockchain technologies and banking high risk entities such as cannabis related businesses. He has worked in the financial services industry for FIS, PayPal, NICE Actimize, and Aite Group and has been quoted by such publications as *American Banker, Bank Info Security, The Times of London, Forbes, The New York Times, and Wall Street & Technology.*

About RegSmart

RegSmart offers the best-in-class automated BSA/AML risk assessment. Supported by subject matter experts, RegSmart collects data with intuitive wizards and stores that data for regulatory compliance and

change management. RegSmart delivers complete, plain language reports with actionable intelligence. Please visit us at www.beregsmart.com.