

Three Threats That Can Harm a Cannabis Business: Cyberattacks, Fraud and Non-Compliance

By Mark Bednarz, CPA, CISA, CFE, Partner

Board members and company executives know the importance of preserving an organization's reputation and taking action to safeguard it from threats. Having a positive image can help drive value for a cannabis business. Conversely, news of a negative event can spread like wildfire and require management to implement costly crisis management procedures to deal with the aftermath.

Failure to properly respond to events in a timely manner can adversely impact investor value and quickly erode customer loyalty. These three threats can put management's business strategy on hold: cyberattacks, fraud risks, and non-compliance with federal and state laws and regulations.

Cyberattacks

The overwhelming number of cybercrime incidents has forced companies to evaluate their information technology environment from a security and resilience standpoint. There are a number of attack vectors that can result in a cybersecurity breach, which can lead to unauthorized access to sensitive information and even the extortion of payment (e.g., ransomware demands). Management and those responsible for the information technology function must work together to develop a cybersecurity risk program, identify the different threats they may face, determine what mitigating controls are already in place, and address the gaps that exist. Due to limited IT staff and complexity of the IT environment, management should consider using a firm that can support the company's IT security needs.

While organizations implement policies, procedures and technology solutions to harden their network and systems, employees tend to be one of their weakest links. Providing periodic security awareness training and conducting simulated phishing campaigns are two inexpensive, yet effective, ways to arm employees with the knowledge necessary to combat these threats and the understanding of how their actions can create business vulnerabilities.

Fraud Risks

Given federal guidelines regarding the cannabis industry, most financial activities occur outside of the banking system. As a result, the cannabis industry has a high reliance on cash transactions, which significantly elevates the level of fraud risk because a "bad actor" – such as a rogue employee – can access the funds of the business. Incidents of fraud can have both a financial and reputational impact to a business because the amounts lost may not be recovered and investigations are costly, disrupt operations, reduce customer trust, and distract management.

Establishing an effective internal control environment can help deter fraud from occurring. A fraud risk assessment should be performed and reviewed annually, unless there are changes to the business strategy, staffing, processes, and technology that warrant more frequent updates. In performing this assessment, the company should involve process owners from different departments and brainstorm the different fraud schemes that could occur by function or process, identify where control gaps and weaknesses exist, and what changes are required.

Leveraging the Integrated Framework for Internal Controls of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission provides a structured, principles-based approach to implementing internal controls within an organization and considers the financial, operational and compliance elements. While “bad actors” will always find new and creative ways to commit fraud, applying the 17 COSO principles to the company’s internal control environment can increase the likelihood that fraud can be prevented or detected.

Non-Compliance with Laws and Regulations

Maintaining compliance is important in the cannabis industry and management must deal with a plethora of requirements, such as strict accounting rules, seed-to-sale tracking, and federal and state laws and regulations. In addition, accountability, data integrity, and dependence on service providers are other factors that increase the complexity of adhering to applicable legal and regulatory guidelines.

According to Allison Kopf, Founder and CEO of Artemis, "Compliance in the cannabis industry is a way to demonstrate accountability to consumers. When you protect your customers, you protect your business. In this rapidly shifting regulatory environment, tomorrow may bring completely new compliance concerns. Creating a robust compliance program with a process for handling regulatory uncertainty strengthens the stability of your operation."

A compliance program should be designed to establish a culture that promotes prevention, detection and resolution of conduct that does not conform to government regulations as well as each company’s own policies and procedures. Establishing a “three lines of defense” model can help structure an effective compliance and risk management program, which senior management and the Board should oversee. Under such a model:

- Operations Management owns and manages the compliance program.
- Risk Management, Compliance and Legal departments oversee the process
- Internal Audit provides the independent assessment as they review the different auditable areas.

Recap

Sustaining a strong governance posture and an effective internal control environment are essential to cannabis businesses that operate in a cash-centric, high profile industry that is subject to the forces of change, the watchful eye of federal and state authorities, and draws the attention of the media and other interested parties. Business owners, the Board and management should be mindful of the need to combat cyberattacks, remain compliant with applicable laws and regulations, and prevent fraud. They should take advantage of the feedback provided by the independent assessments performed by a company’s external financial statement auditors, cybersecurity specialists, internal auditors, and risk management specialists.

Staying focused on managing risk is critical to overall business success.

Contact Us

For more information on how PKF O’Connor Davies, LLP can assist your business in managing risks associated with cyberattacks, fraud and non-compliance with laws and regulations, please contact:

Mark Bednarz, CPA, CISA, CFE

Partner

mbednarz@pkfod.com | 973.216.5950

About PKF O’Connor Davies

PKF O’Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, eleven offices in New York, New Jersey, Connecticut, Maryland and Rhode Island, and more than 700 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O’Connor Davies is ranked 29th on *Accounting Today’s* 2019 “Top 100 Firms” list.

PKF O’Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.

Our Firm provides the information in this e-newsletter for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.